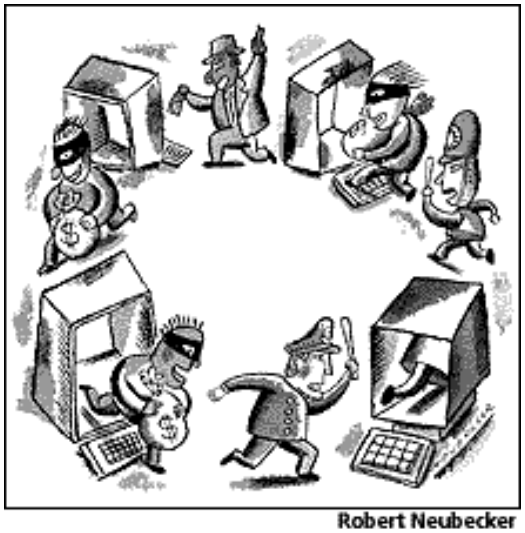
Security for Notebook PC Wireless Communications

802.11, Bluetooth*, WWAN, …

Background Tutorial and Guidelines



Robert Neubecker

July 2002
Revision 1.0b

Intel Corporation

Contents

FIGURES

Revision History

Rev.	Description	Date
1.0a	First document release	July 2002

1 Wireless PC Communications Security Overview

The purpose of this document is to provide background information, recommendations and guidelines for software support used with wireless communications devices in a notebook PC for both corporate, small business, and consumer use.

1.1 Introduction

Platform security is critical to ensure the trust and confidence users have for keeping data safe both within the computer as well as when it may be transmitted across a communications channel to another user. Safe computing is a necessity in moving the computer industry forward and is complimentary to the pillars of mobile next generation notebook PCs defined by Intel. The need to protect user data and secrets is prevalent in wired communications on corporate networks and Internet traffic, and is amplified in a wireless communications environment where data is prone to other security threats.

Wireless networks are now becoming widely deployed, and manufacturers have accelerated the development of low-cost, interoperable products. Today's 802.11 wireless technology promises to open up exciting new possibilities. Other wireless communications technologies enhance the ability for users to access data almost anytime and anywhere. However, as wireless communications solutions become more numerous and widespread, more robust security solutions are required.

Wireless networking is a natural extension to a company's wired network. High-performance, wireless solutions can greatly increase an employee's productivity by providing real-time access to e-Business applications and valuable networked data. Most enterprise applications are designed and deployed for use on network-connected personal computers. Users who are unable to access needed applications, wherever and whenever they need them, typically experience a wide range of difficulties. These can include delays in responding to customer requests, dissemination of inaccurate information, and delivering lower-quality work output. For example, a professional sales force with a mandate to spend the majority of its time in the field with customers may have access to a networked workstation and e-Business tools for Customer Relationship Management (CRM), but only for a small percentage of the work day. With mobile access to applications such as CRM, order management, e-mail, and intra/Internet access, the sales force can have the advantages of real-time information delivered at the customer site. The required investment in wireless infrastructure may result in productivity benefits, improved competitive standing, and customer affinity that could add up to a measurable monetary impact. The Mobile office gives employees secure access to their information, applications, and teams — anytime, anywhere— so they can get their job done whether they are at work, at home, or on the road.

Mobility at work makes employees more productive. Whether they are in a large headquarters office building, a small sales office, or in a manufacturing or other specialty location, giving workers real-time access to information is key to increasing productivity and corporate profitability. In today's enterprise work environment, with globally dispersed work teams, employees are spending less time fixed to their desk and more time roaming around offices on a corporate campus, in collaborative work meetings, telecommuting, and working in remote locations to accomplish their job objectives. While they are spending less time fixed to the desk,

they still need network connectivity to do their jobs. Wireless LAN and mobile notebooks keep these workers connected to their data and teams. Providing secure mechanisms to match the mobility aspects is a critical aspect not to be overlooked.

Breaches in data security through computer connections are a reality of doing business. Whether it's a computer virus that an unsuspecting employee triggers or a denial-of-service attack successfully executed, security incidents happen. According to a May 13, 2002 article in InformationWeek[1], computer crime is expected to grow by 230% during 2002 mixed with the growth of computer virus attacks increasing by 22% during the same year. Companies need to cover all aspects of computer security to reduce these risks.

The ultimate goal is to fortify wireless network security by implementing and utilizing technologies to provide the safe computing environment that every user expects, regardless of location or method to connect back to the corporation. Many security technologies provide the means to enable secure communications. Technologies discussed in this document include client firewall and intrusion detection software (IDS), virtual private networking (VPN), secondary authentication, virus controls, as well as specific discussions for 802.11 wireless LAN, Bluetooth*, and WLAN.

This document addresses several aspects of security concerns, provides guidance to counter such concerns, and provides recommendations for implementation of solutions. For the critical security needs, solutions exist and the same client solutions can be used to span all virtual "office locations" of the mobile user.

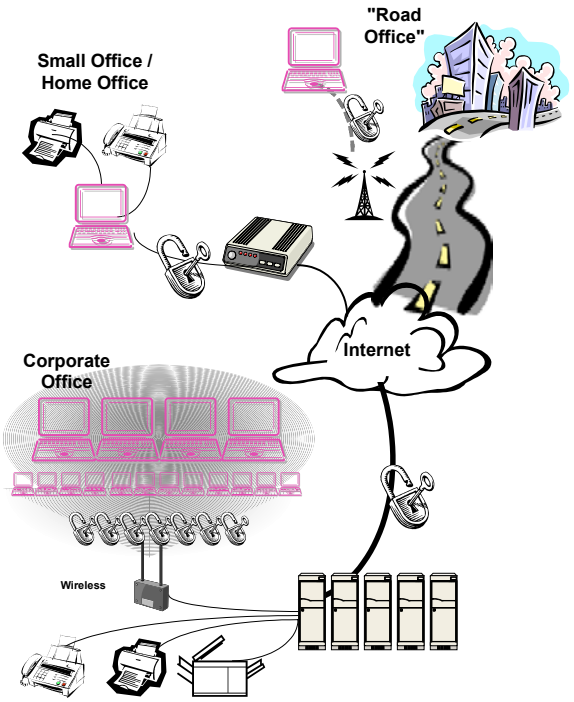


Figure 1: Same Security Solution Spans All Office "Locations"

[1] Information Week, May 13, 2002: "Batten Down the Security Hatches" by Helen D'Antoni. http://www.informationweek.com/story/IWK20020509S0003

1.2 Audience

The intended audience of this document includes both technical implementers as well as decision makers within the following areas:

- Wireless communications hardware engineering
- Software engineering for wireless communications devices
- Middle-ware software for communications stacks
- PC OEMs who will provide wireless communications devices for their platforms

2 Foundations for Security Solutions

The basis for security solutions of course depends on the type and classification of threats posed to computer data as it resides on the PC as well as data that is transmitted across any sort of communications link.

2.1 PC Security Threats

Security breeches of enterprise information systems are on the rise. Figure 2 below shows a dramatic level of cybercrimes committed against various companies as reported by the FBI/CSI Computer Crime and Security Survey. In some categories, such as virus attacks and insider abuse of network access, the numbers are relatively large. In other cases such as theft of proprietary information, the numbers may seem small, but remember that a single theft of secret information can be devastating to any company regardless of the size or stature of the institution.

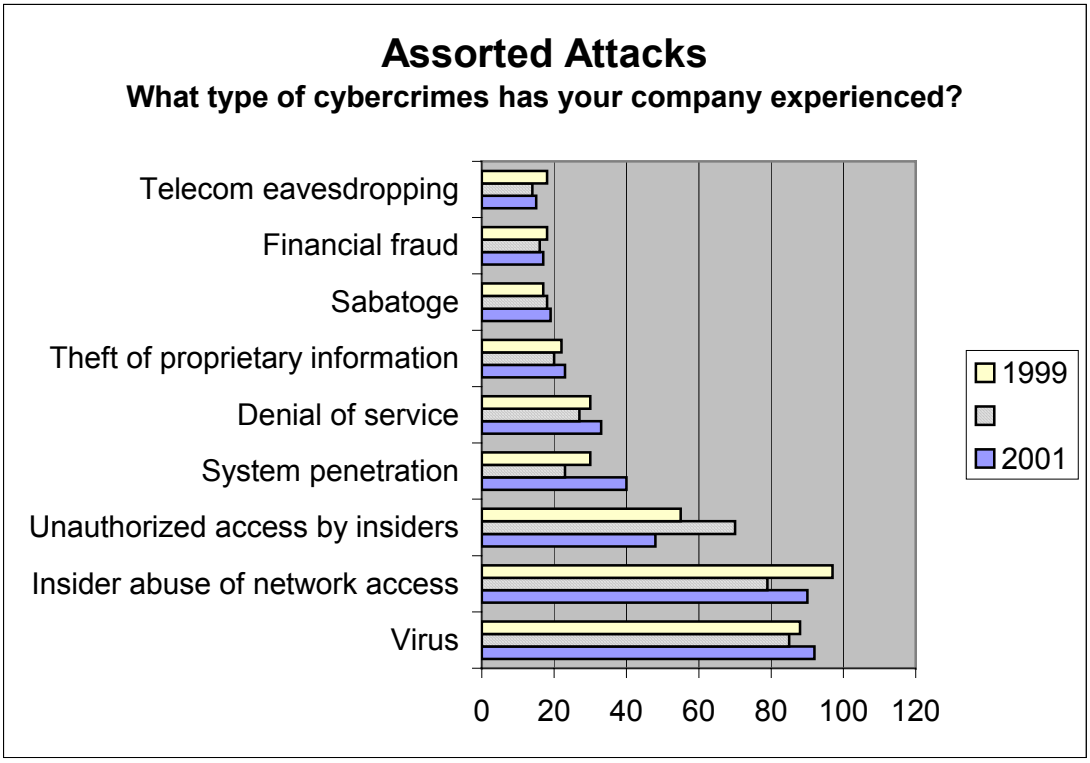


Figure 2: Cybercrimes[2]

Whether attackers want to commit information theft and fraud, disrupt business operations or simply prove a point, they have many ways to do damage:

- Destroying files and applications via a virus, Trojan horse, worm or other malicious code.
- Gaining access to systems and network by cracking or stealing passwords, eavesdropping electronically, or manipulating networking protocols.
- Shutting down a Web site through a denial of service attack.
- Impersonating a trusted system (spoofing) or a user (e-mail hacking or identify theft).

Just as security threats continue to increase, so also is corporate spending on security solutions. And although no security technology is bulletproof, a multi-layer approach to information security is the best strategy—and powerful client PCs play an important role in building a secure infrastructure.

From this discussion, notebook computers are exposed to several security threats that can be broadly classified into two categories: theft or damage to data residing on the computer and theft or damage to data as it is transmitted across any sort of communications link.

Threats to Data on Local PC. This threat arises from the fact because of the mobility factor of a notebook PC, they are more prone to be stolen than their desktop counterparts. It is often found

[2] Base Respondents: 1999 = 460; 2000 = 583; 2001 = 484. Source: FBI/CSI Computer Crime and Security Survey of Computer Security Practitioners

that the stolen data is more valuable than just the cost of the notebook hardware. Furthermore, notebooks can be subject to a variety of hardware as well as software attacks.

Data communication attack. Notebooks use various means of communication to access the corporate network or the Internet and often operate outside of corporate firewalls. There are a number of ways in which a determined hacker can attack the communication channel used by the notebook to steal the data being transceived.

The table below captures the various threats under major categories. The list is not intended to be exhaustive, but to provide some sense for security concerns that exist.

Table 1: Data Security Threats

Threats	Current Solutions	Weaknesses
Data theft	Data encryption (EFS, VPN, encrypted email, etc.)	Encryption keys are stored on the hard disk and are susceptible to tampering
Unauthorized access to platform	1. Username / Password 2. Biometrics and external tokens for user authentication	1. Subject to dictionary attacks 2. Biometrics can be spoofed 3. Authentication credentials not bound to platform
Unauthorized access to network	Windows network logon, IEEE 802.1X	1. Can be bypassed 2. Certificate can be spoofed 3. Authentication data is stored on the hard disk and is susceptible to tampering
Virus	Virus detection software	Difficult to keep up with viruses as they come out

A variety of solutions exist today to address the plethora of security concerns. Many solutions exist which could have possibly eliminated some of the instances of crimes shown in Figure 2 and the broad categories shown in Table 1 above. In some cases, the security solutions aren't presently strong enough alone to solve the existing concerns. Although the solutions to address current security concerns exist, they alone may not be strong enough and new security threats may render existing solutions ineffective.

The foundations used to address security concerns are based on three general types of security solutions that will be discussed in this paper along with examples associated with respective wireless communications technologies. These solutions fall into these categories:

- **Software only security.** Security solutions can be implemented using standards based software algorithms running on the PCs host processor without additional specialized security hardware to assist.
- **Security provided by removable security devices (with software support).** This group includes any hardware security device that is not permanently fixed to the computer such that it is intended to be plugged in and removed by the user. The most common example is a smart card.
- **Security solutions based on security devices fixed to the motherboard of a PC (with software support).** This category is best represented by the Trusted Platform Module (TPM) as defined by the Trusted Computing Platform Alliance, an industry group focused on providing infrastructure for solving security concerns. Security devices in this category are permanently soldered and/or glued to the notebook motherboard.

2.2 Software Only Security Solutions

Security solutions can be provided to improve the robustness for data integrity both on the PC and as it is transmitted to other machines through use of standards based software solutions. Encryption algorithms are available in Windows 2000* and Windows XP* through MS-CAPI (see section 3.1.1 for more details). This software interface provides access not only to hardware encryption devices on the platform, but can also provide software-only encryption implementations.

VPN is an example of a software security solution on a client notebook PC used to provide an encrypted communications channel from one machine to another, potentially including a wireless leg of the connection that could also include the Internet as the medium. VPN software solutions also deploy with part of that infrastructure solution on the enterprise server side of the connection within the corporate enterprise. VPN traditionally uses software encryption to create the trusted link, a point to point encrypted pathway where data can be safely transmitted . Depending on the particular vendor providing the VPN software, the encryption and authentication methods used may take advantage of software standards (such as MS-CAPI) or may be done through totally proprietary methods. It is best to utilize software standards for encryption and authentication which enables software such as VPN to use whatever strong security methods are available on the system. For example, a VPN using MS-CAPI interfaces for encryption could have encryption done using a TPM (hardware security device) which can be stronger and more secure that encryption done through software alone.

Although software encryption provides a great improvement over “no encryption at all”, it is still prone to attacks and discovery from software intent on spying and theft. In the case where software-only encryption is used from any software entity, there is a risk that encryption keys can be stolen by malicious software within the operating environment. Other authentication certificates or encryption keys are stored on the hard disk of the computer. Doing so increases the risk of denial of service attacks wherein malicious software can simply delete those files which can disable the user from gaining access to services provided by those files.

2.3 Removable Security Devices

Removable security devices take on a wide variety of sizes, form factors, functions, and intended uses. Among the most common within the category of removable security devices is the smart

card. Relatively new form factors for related function devices includes USB security tokens and USB SIM cards. All removable security devices offer "two factor authentication": something you have (the device) and something you know (the PIN to unlock secrets stored on the device). These devices are capable of storing authentication certificates used to authenticate to networks or computers, but can only be accessed when the user enters his PIN to release that information from the device.

There are a variety of security issues that are improved through the use of hardware security devices where secrets can be safely stored and revealed only for authentication purposes. Removable security devices include support to store such authentication keys along with private keys used for encryption of wireless data transmissions. The alternative to using hardware security devices to store secrets is to use the "certificate store" provided by Windows. Implementation for Windows* 2000 and Windows XP, this certificate store is found in a folder on the default hard disk. In this storage location, these certificates have no protection.

Use of removable hardware security devices can safely store secrets used for user authentication. For example, Windows XP* has built-in support for 802.1X to improve the user authentication process for wired and wireless network connections. The Windows XP* implementation further enhances this mechanism by providing support to store and retrieve authentication certificates in removable security devices such as smart cards or USB security tokens. In fact, any hardware security device can be used to store such authentication certificates as long as that device has a compliant CAPI software interface.

In general terms, all removable security devices interface to application software through standard APIs including MS-CAPI and PKCS#11. A specific layered software stack may also be defined as general purpose method of communicating to the hardware, such as the PC/SC (PC Smart Card) interface. All such industry standard software interfaces to the hardware are provided by the hardware vendor.

2.3.1 Smart Card

A "smart card" is a plastic credit card with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a PC. It is more secure than a common magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. Most commonly used in European countries as a financial card, it also can provide security functions needed for safer personal computing.

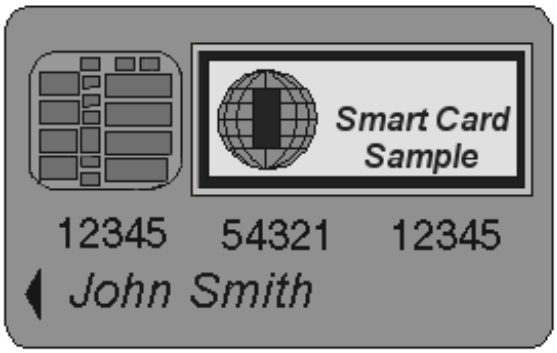


Figure 3: Smart card

Smart cards provide security functions when plugged into a notebook PC. Organizations and corporations using PCs for business and communication can take advantage of a smart card for its security functions to store important data and for its encryption capabilities. Smart cards can make private information readily available to those who need it, while at the same time protecting the privacy of individuals and keeping their informational assets safe from hacking and other unwanted intrusions. In this capacity, smart cards enable:

- Secure logon and authentication of users to PCs, wired networks, and wireless networks
- Secure B2B (business to business) and B2C (business to consumer) e-commerce
- Storage of digital certificates, credentials and passwords
- Encryption of sensitive data

The key advantage of using a smart card for PC security is that it provides secure storage for valuable information such as private keys, account numbers, passwords, personal information, and certificates used for authentication. Information stored on a smart card is only released upon user approval, generally in the form of a dialog box that prompts for a PIN to access smart card data. If the user enters an invalid PIN, the smart card can be pre-configured to deny all subsequent access.

The smart card is also a secure place to perform processes that shouldn't be done "exposed to the world," for example, performing a public key or private key encryption. Encryption keys can be generated by the smart card with the private key stored on the smart card. The private key can be used for encryption and hashing without ever being released from the smart card into the host operating system where it could be compromised or stolen. This is an additional benefit over software only security solutions.

Smart card readers attach to the notebook PC via either USB or PCMCIA and come in a wide variety of form factors and price ranges. Both smart cards and smart card readers are available from many vendors.

2.3.2 USB Security Token

For applications that need a form factor different than a smart card, the same functionality of a smart card is also offered on devices generically called "USB security tokens" or "Smart tokens". This class of device offers user authentication, digital signatures, and data privacy all in a familiar key-sized token. They are technologically identical to smart cards, have a different form factor that is about the same size as a house key, and plug into the USB port of a notebook computer. Figure 4 below shows a USB Security Token with a house key for size comparison. The advantage of this class of device is that it does not require a separate reader – the reader and the security functions are bundled together into a key fob device.

Figure 4: USB Security Token (with house key for size comparison)

Just as with the smart card, this class of device is a portable vault for private keys and other digital secrets like biometric templates, passwords, personal information, and e-cash. Storage on these devices can be up to 32Kbytes. It also provides encryption and hashing methods similar to smart cards.

Because these devices are removable, they provide storage for information that needs to be portable and associated with the user as the user carries this device. When secure information is needed, the device is plugged into the computer's USB port for retrieval. Depending on the application and configuration, the device can then be removed from the PC. Because it is removable, it is designed for storage of information tied to the user (such as user authentication certificates) rather than information that is intended to be tied to the computer itself.

The USB security token is capable of performing all private, public, and secret key functions within the token. When these critical operations are performed within the security token, a much higher level of information security is achieved than can be provided by client-side software-only solutions. Just as with the Smart card, the performance of the onboard security processor is small and large scale encryption and decryption within the device can be very slow. It is up to the particular application to chose whether the functions should be performed within the device or within the supporting software stack using the power of the computer's host processor.

2.3.3 USB SIM Card & Reader

A third form factor of removable security devices for smart card capabilities is offered through a tiny SIM-size smart card and reader. This class of removable security device offers removable cards that are the same size and shape as SIM cards compliant with the GSM 11.11 specification. These tiny form factor cards are fully compliant with standard smart card definitions, just smaller measuring 25 x 15mm. The reader for the tiny smart cards provides a USB connection to the PC measures ~65 x 20 x 10 mm as shown in Figure 5 below.

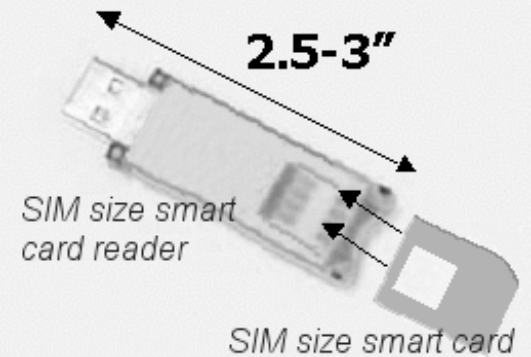


Figure 5: SIM size smart card and reader

These devices are available from several vendors to provide the same technical functionality as a smart card or USB security token, just with a different form factor and flexibility. They offer non-volatile storage and on board encryption/hashing which can be used to store private information such as user authentication certificates, passwords, and other secret data, along with the private keys used for encrypting data.

The tiny form factor smart card that is plugged into these readers is tightly coupled once inserted into the USB reader such that it won't fall out. Some product implementations provide a mechanical latch to more securely hold the tiny smart card into the reader. The tiny smart card may be removed by reversing the mechanical latch to release the card. In many cases, the usage model may be to keep the same card in the reader at all times, and rarely remove it. Other cases may require changing the SIM card for various usage needs.

2.3.4 Which removable security device is right?

As discussed in previous sections of this document, the technical capabilities of removable security devices are equivalent. Of course, a manufacturer may choose to add or replace a particular feature to provide value-add in order to distinguish that product from others in the market, but they basically all provide the same thing. So how do you choose one device over another? Just as you would make careful decisions before purchasing a new television for your family room based on a wide variety of choices, each offering basically the same thing albeit with various sizes, shapes, prices, and features to distinguish from other products on the market -- the decision for the basis of security solutions must be made carefully in order to get the right solution for specific business needs.

Selection of which type of device is right depends on a number of factors. In all respects, ease of use, reliability, tamper resistance, vulnerability, flexibility, functionality, software support, and acceptance can be considered the same for all types of removable security devices. There are a few topics where these classes of devices are different: form factor and cost.

- **Form factor.** Smart cards require that a separate reader be added to the notebook computer, generally attached to either the USB port or through the PCMCIA slot. The size of the reader is approximately the size of a deck of cards with an attached cable that is approximately 1M in length. The actual security electronics of the smart card is in the card itself (not part of the reader) which can be made part of the standard corporate identification badge or a separate card that is kept in the user's wallet. The USB security tokens are small and self contained. No extra reader is needed. The USB security token

can be kept on a key chain or with the user's corporate ID badge. PC SIM card readers are similar in size and shape to the USB security tokens, but offer some advantages to having a separate card used in that tiny reader.

- **Cost.** Smart cards are relatively inexpensive. The smart card reader is somewhat more expensive, but volume pricing is available from the hardware vendors. Smart cards have been in existence for many years, so you can expect the technology to be pretty standard and cost should lower over time. USB security tokens are fairly new to the security market and hence the pricing probably won't come down because volumes are still relatively low and the technology is still new.
- **Software.** Selection of a specific device should also include careful evaluation of the software support provided by the vendor. Not all vendors provide the same level of software support for the user side of the connection or the enterprise corporate management side of the device. This evaluation is just as critical, if not more so, than the selection of the form factor of the device.

2.4 TPM Based Security Solutions

The TCPA's 1.1b specification, published in February 2002 (available from the group's website at http://www.trustedcomputing.org), defines a PC subsystem that supports trusted processes and transactions. A TCPA-compliant platform performs cryptographic calculations, provides platform-level authentication and protects against security breaches during electronic transactions and communications. The silicon implementation of the TCPA definition is called the Trusted Platform Module, or TPM

During the process of defining a new security standard, the TCPA forum came to an important conclusion: the level of trust they were able to deliver to PC users needed to be increased and security solutions for PC's needed to be easy to deploy, use and manage. The level of trust of the PC has a critical role in the continuing information revolution wherein the PC and the Internet are the cornerstones. With that in mind, industry leaders formed the TCPA working group to create definitions to improve the level of safe computing for today and for coming generations of PCs.

- The development of the Trusted Computing Environment will set the framework to enable e-business practices and e-commerce transactions to occur.
- TCPA is an industry alliance focused on enhancing trust and security on computer platforms.
- Intel is enabling the industry to develop corporate and consumer products that support TCPA specification version 1.1b
- Intel sponsors the TCPA to enable fundamental criteria for e-business and e-commerce adoption.

The TCPA defined what is called the Trusted Platform Module, or TPM, with the intent to provide for improved trust in the PC platform. A Trusted Platform Module is a hardware device that is connected to a platform's motherboard and is used to validate the identity and operating parameters of a computer or device used in a trusted computing environment. The TPM security subsystem, a combination of hardware and software, helps protect user authentication and both wired and wireless communications. The TPM and the data stored within it are isolated

from all other components on a platform. In addition, TPMs aren't interchangeable between platforms. TPMs protect users' data by generating a distinct digital signature that verifies the exact platform and hard drive from which data is to be accessed.

In broad terms, the functions provided by a TPM fixed to the motherboard of a notebook computer can be viewed the same as a smart card securely attached to the PC. The TPM provides the same level of encryption, secure storage, and cryptographic functions as are provided by other removable security devices, with more functionality rolled into it as well.

Not only does the TPM provide the standard crypto functions / features including non-volatile storage, encryption and hashing, random number and key generation, but also the TCPA specification further defines a means of determine if the configuration of the system has changed. This provides a mechanism to determine if a virus or other malicious software has infected the system within the operating environment or even through a firmware "update".

1. The Trusted Computing Platform Alliance (TCPA) defines a hardware device that is attached to the platform, as a Trust Platform Module (TPM).
2. Once the data is sealed inside the TPM with a storage key, the sealed data can only be accessed from this hard drive with this platform configuration.
3. If the TPM recognizes that a system has a different configuration, such as booted with a different operating system, access is denied.

Figure 6: TPM Security

Software interfaces to the TPM are provided for application software and middleware to access cryptographic functions of the TPM. In the runtime environment of Windows*, hardware vendors for the TPM generally provide software interfaces for MS-CAPI, PKCS#11, and TSS (TPM Software Stack). Versions of these software interfaces are provided by the TPM vendor. Additional information regarding safe computing provided by TPM's used for notebook computers can be found in an Intel white paper titled "Trusted Platform Module (TPM) based Security on Notebook PCs".

3 Common Security Infrastructure for Wireless Communications

There are a variety of common security building blocks that, when properly installed and configured, can be used to alleviate concerns about safe computing. Data within the computer as well as data transmitted across wired or wireless communications links can be kept secure.

3.1 Software Cryptographic Interfaces

In order to take advantage of the cryptographic functions found on hardware security devices such as a TPM or smart card, a software interface must be provided so that higher level software can use those functions/features of the hardware. Higher level security tools, applications and middle-ware, are written to take advantage of these software APIs to provide a reliable security solution. Software interfaces have been defined, published, and developed to provide standard function interfaces for applications to use functions of both hardware and software-only crypto solutions. Although there are a plethora of such "general crypto APIs" published, a few have gained broad acceptance for use on notebook PCs using flavors of the Windows* operating systems. These include: Microsoft Cryptographic API or CAPI; PKCS#11 or Cryptoki API; and the TCPA Software Stack Specification (TSS).

3.1.1 Microsoft Crypto API (CAPI)

Several crypto software API standards have been created, each varying in their degree of modularity, sophistication, cryptographic transparency, and proprietary content. To minimize development costs, licensing fees for algorithms, and the potential for unsafe programming, a standardized interface to cryptographic functionality -- a CAPI or Crypto API (Cryptographic Application Programming Interface) -- was defined and implemented by Microsoft. Most cryptographic functions within the Microsoft* operating system environments are based on MS-CAPI. It provides a standard software API to interface to various security services. The architecture is modular and extensible to accommodate emerging technologies, allowing developers to update their applications to the latest security services at low cost and minimal effort.

MS-CAPI provides a software interface to allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. The general architecture for MS-CAPI provides a modular approach so that "plug-in" modules provide all cryptographic operations. Each independent module is referred to as a *cryptographic service provider* or CSP.

As shown in Figure 7, MS-CAPI functions as an intermediary between applications and CSPs. Specifically, the MS-CAPI allows applications to perform cryptographic operations using keys and credentials while controlling and restricting access to the sensitive data contained within CSPs. Microsoft provides several software-only CSPs, such as the RSA Base Provider and the Strong Cryptographic Provider -- a.k.a. the Enhanced Cryptographic Provider. These software-only CSPs are included with Windows 2000* and Windows XP.

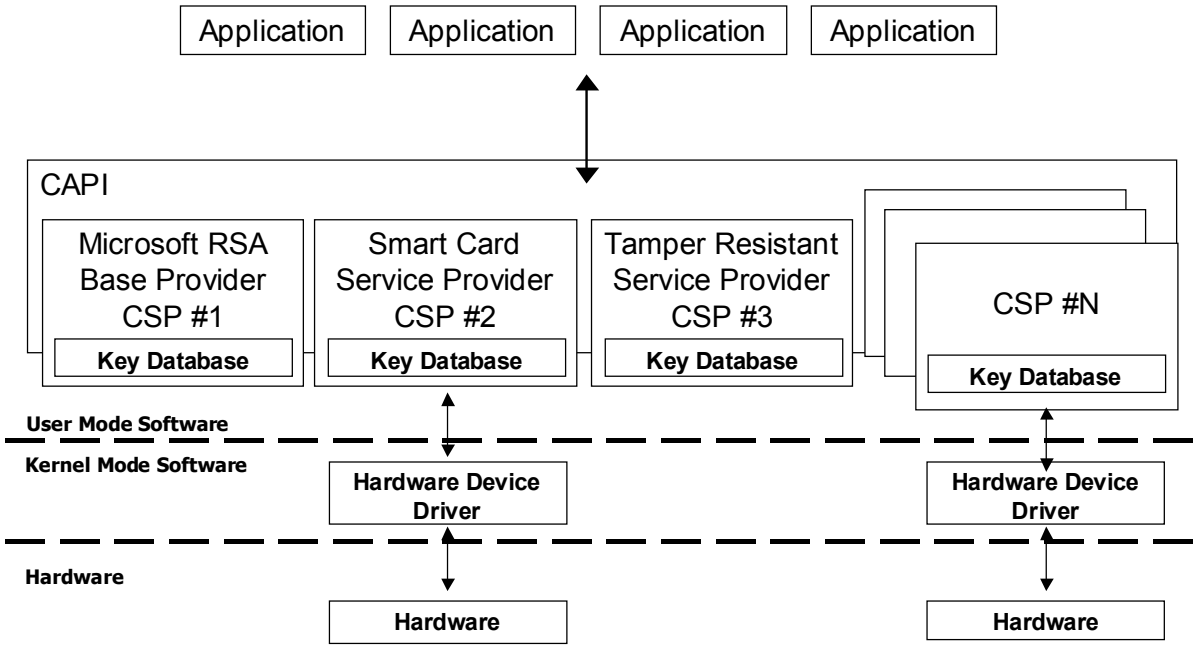


Figure 7: MS CAPI Block Architecture

As MS-CAPI is designed to accommodate enhancements to cryptographic functions, other CSPs can be installed and registered on a PC. Each CSP provides a unique implementation of the Cryptography API layer with various features, cryptographic strengths, flexibility, and other improvements. For example, a CAPI CSP may provide stronger cryptographic algorithms, while others provide an interface to security functions provided by a hardware device such as TPM or smart cards. Along with the varying levels of cryptographic strength come different legal restrictions (such as licensing and export). Modular CSPs can easily be interchanged to meet such restrictions. CAPI CSPs may optionally present status and solicit input from users via some form of user interface. For instance, a CSP may prompt for the user to enter a PIN before providing digital signatures generated using the user's signature private key found on a hardware token such as the TPM.

Vendors providing hardware security devices such as the TPM, USB security tokens, or smart cards provide their own software interfaces compliant with Microsoft's CAPI definitions. These CAPI CSP interfaces are distributed by the hardware vendors with their products with a mechanism to install the software to take advantage of the hardware security functions by any software application written to use MS-CAPI.

Version 2.01 of the MS-CAPI specification is the latest release. Additional information regarding MS-CAPI software interface is available from Microsoft's website.

3.1.2 PKCS#11

PKCS#11 (Public-Key Cryptography Standard 11), sometimes referred to as "Cryptoki" (pronounced crypto-key), is one of the PKI family specifications defined and delivered by a consortium headed by RSA Security*. The PKCS#11 software interface deals with the storage of certificates and cryptographic functions on hardware security devices to provide a interface for multi-platform, crypto-aware, driver-level software API. PKCS #11 isolates application software by facilitating the use of hardware security devices that work with cryptography,

including smart cards, USB security tokens, and TPMs. It is well suited as an interface to such hardware security devices as well as other cryptographic accelerators, as well as those used to speed up Secure Sockets Layer (SSL) or IP Security protocol (IPSec) processing. PKCS #11 is a multi-platform standard available under Apple*, Linux*, Unix*, Windows*, and other operating environments. Figure 8 below depicts the high level, block architecture of PKCS#11.

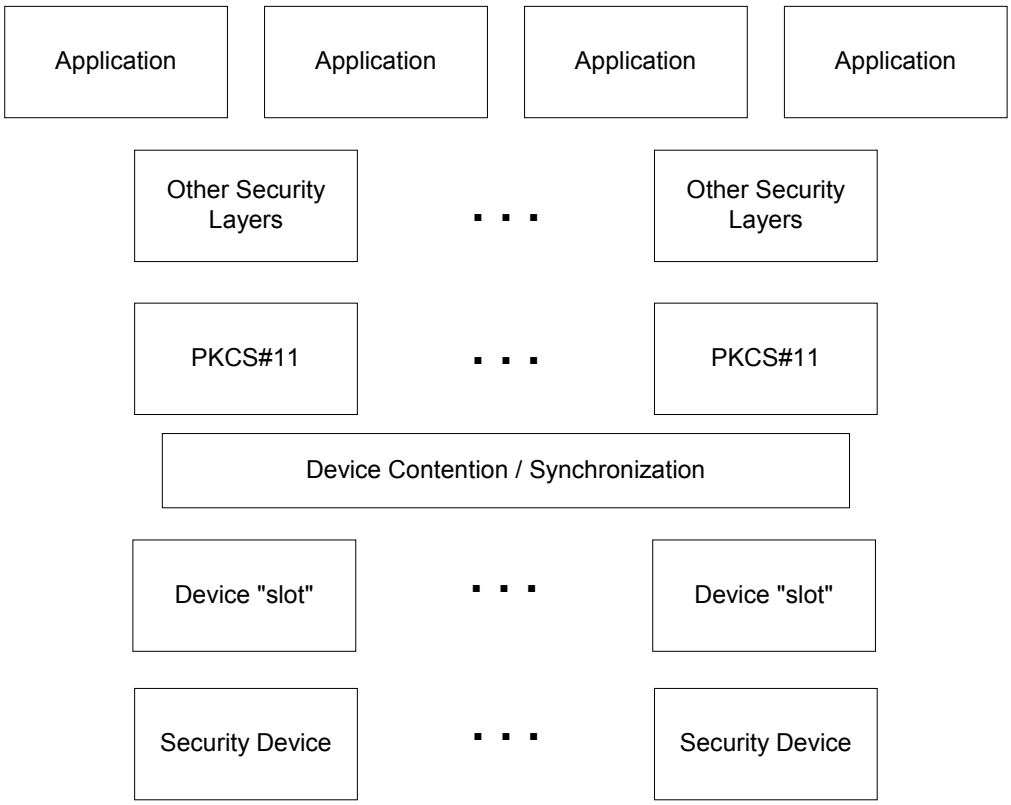


Figure 8: PKCS#11 Block Architecture

As shown in Figure 8, PKCS#11 provides a software interface from an application program to security devices available in a given system through a number of "slots". Each slot corresponds to a given security device and is functional when the device is present. For example, a "slot" may exist for a smart card reader but is only accessible to application software when a smart card is inserted into the reader. Any number of security devices as shown in the diagram may in effect be a smart card or TPM or some other crypto hardware. It is possible that a number of slots may be associated with a given smart card reader with the understanding that a single reader can provide access to any number of different smart cards. In the case of a TPM or other fixed security device, PKCS#11 provides only a single slot to that device. Each device is made to look virtually like every other crypto device which enables application software to use hardware security devices in a "generic manner" as details of the device are hidden.

The logical structure of this architecture further enables PKCS#11 software to virtualize a cryptographic device totally in software. In the block diagram of Figure 8, the "security device" could be a physical hardware device or it could be a virtualized encryption device implemented totally in software.

Cryptoki Version 2.1 is intended for cryptographic devices associated with a single user, so some features that might be included in a general-purpose interface are omitted. For example, Cryptoki Version 2.1 does not have a means of distinguishing multiple users. The focus is on a single user's keys and perhaps a small number of certificates related to them. Moreover, the emphasis is on cryptography. While the device may perform useful non-cryptographic functions, such functions are left to other interfaces.

PKCS#11 and MS-CAPI have similarities and differences. PKCS#11 is similar to MS-CAPI in that they both provide abstraction layers for cryptographic functions that can be tied to security devices, both hardware and software implementations. This enables application software to use crypto functions without the need to know details about the specific crypto device being used. The sole difference between MS-CAPI and PKCS#11 is that despite the similar intent, they are defined by two different forums. As such, even though the software provides fundamentally the same functionality, the interfaces are not the same. Hence, an application written to use PKCS#11 cannot expect to use MS-CAPI without additional code to support the other crypto interface.

Netscape client and server software is the most common example of PKCS#11 use. Other software from Baltimore and Entrust also use PKCS#11 for cryptographic functions. Don't consider this short list to be all inclusive: there are certainly others.

As with the MS-CAPI interface, most hardware security device vendors provide software support for PKCS#11 with their hardware deliverables.

Additional information as well as a copy of the latest version 2.11 specification is available from the RSA website at http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11.

3.1.3 TPM Software Stack (TSS)

The TCPA Main Specification v1.1b provides a hardware component level definition of a cryptographic device with functions intended to increase the level of trust within a computer. This hardware crypto component, the TPM (Trusted Platform Module), necessitates a general purpose software interface to abstract access to the hardware by application software, middleware, and kernel mode services. Just as the TCPA specification is platform agnostic, so also the TPM Software Stack (TSS) definition is written to be indifferent to the type of platform and operating system. The specification can be implemented on any type of computer or device under any operating environment.

The diagram below (Figure 9) shows the general block architecture of the TSS. As point of reference, the TPM hardware is shown at the bottom of the diagram with software device drivers interfacing to the hardware. Modular implementation can provide various other levels in User Mode space to provide the core services and specific additional services to applications and middle-ware.

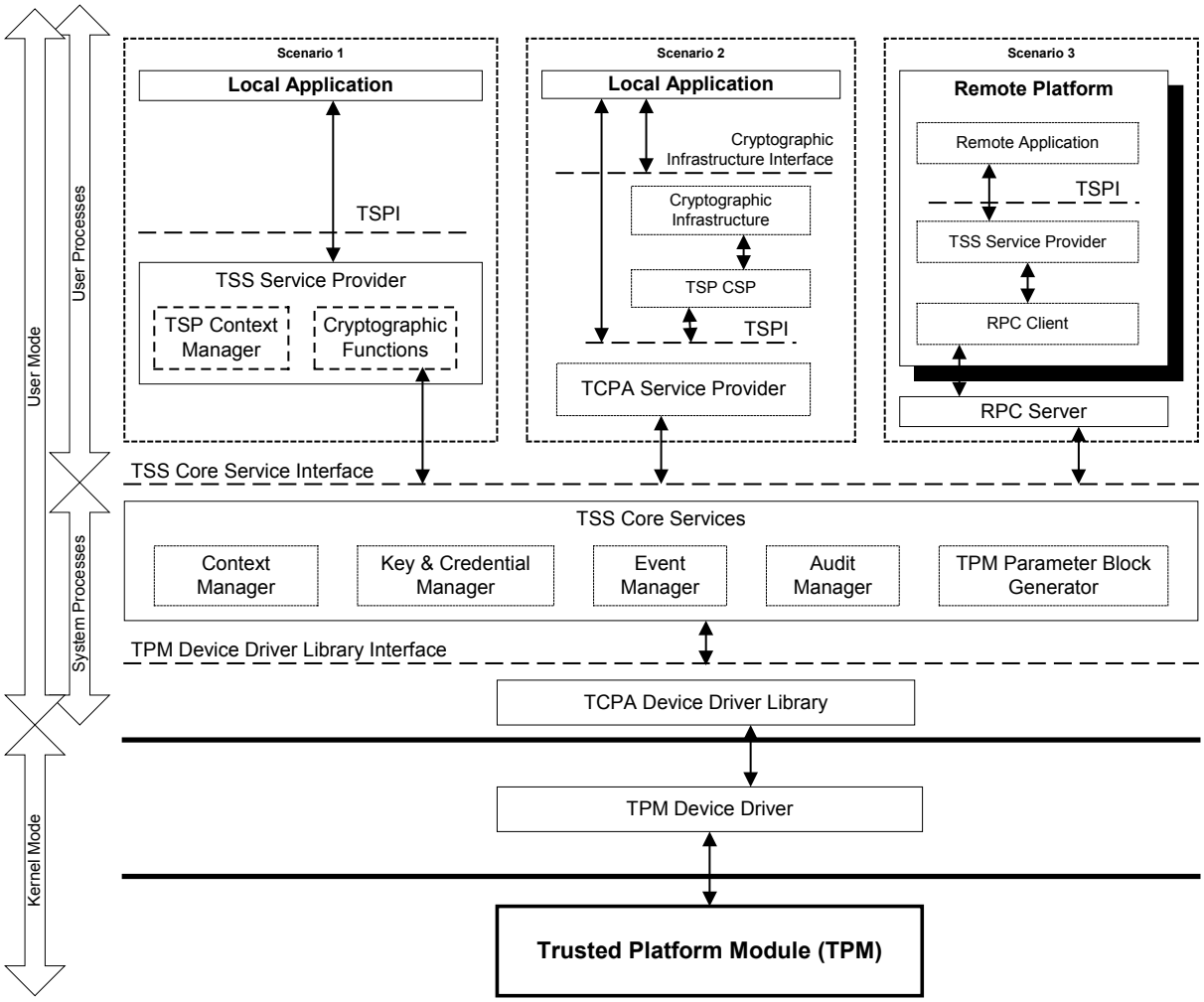


Figure 9: TPM Software Stack Block Architecture

Within the TSS, a Cryptographic Service Provider (CSP) provides encryption capabilities for the system. TSS CSPs provide their functions either solely based on hardware crypto devices (PC add-in card, smart card, other hardware token, etc.), totally software-based, or a combination of both. A TSS CSP typically provides the following functions:

- Data encryption and decryption
- Digital signatures
- Cryptographic hashing
- Key generation
- Random number generation
- Nonvolatile secure storage of private keys

In order to provide data security within the PC and data that is transmitted to and from the PC, there is a need to encrypt and decrypt data. Any data can be protected through encryption and secure storage of the key used for encryption. In the same way, any signing authority can be protected if the signing key is stored in a protect and secure way. The TSS provides a service to

encrypt, decrypt, and securely store encryption keys as the TPM acts as a portal to keep data and keys confidential. “Protected Storage” is a set of commands provided by the TPM through the TSS to enable virtual secure storage space.

In addition to providing an interface to the TPM for encryption, decryption, and secure key storage, the other interfaces are provided through which the TPM can be utilized for hashing, key generation, and random number generation. These functions are all a part of a robust tool set provided by the TPM which can be accessed by application software and middle-ware running in user mode. Software APIs to TPM functions can be provided through registered CSPs for MS-CAPI, PKCS#11, as well as through software calls to the TSS. For example, a compliant Microsoft CAPI CSP interface to the TPM can be defined to install as a certified CAPI CSP entity. In order for this CSP to provide its cryptographic capabilities, it may utilize functions of the TSS as depicted in the middle box of Figure 9.

3.2 Multi Factor Authentication

In addition to the standard hardware and software security foundation blocks described above, there are other important aspects to consider. Whether we realize it or not, multi-factor authentication is part of our every day society. Here are a couple of examples. What about when you’re slaving away at your desk, you’re boss walks up behind you, and pats you on the back saying “Good job!” Although the voice sounds familiar, you are forced to turn to match the face with the voice that you thought was perhaps your boss, but couldn’t be sure without looking. That’s a form of two factor authentication: we match the voice print and the face with who we know. Here’s another example. In the financial world, we present a check with our signature at the bottom (“something you do”), and the clerk asks to match the signature with the signature on our driver’s license (“something you have”) and also matches our face with the picture on the driver’s license (“something you are”). In the electronic world, as we use our debit card to make a purchase (“something you have”), we are required to enter a PIN (“something you know”) to authorize the transaction. We are comfortable with those methods of authentication, albeit redundant, because of the security it provides.

Multi factor authentication for personal computer security takes the form of a combination of two or more authentication schemes: “something you have”, “something you know”, “something you are”, and/or “something you do.” An example of “something you have” takes the form of a smart card or USB security token (or the driver’s license in the example above). The “something you know” is demonstrated by the PIN required to unlock secrets from that hardware security device. The “something you are” is found in forms of biometric authentication such as fingerprint or iris scan matching. The “something you do” is another type of biometric authentication analysis done by signature matching, handwriting analysis, or keystroke analysis.

Security solutions based solely on software do not include multi-factor authentication. Only solutions using an additional hardware device provide the additional level of authentication necessary for a secure transaction that cannot be easily spoofed. Of course, authentication can be extended to multi-factor authentication for enhanced security by adding an additional authentication mechanism to the security implementation, e.g. PIN or fingerprint for user authorization to a smart card which authenticates itself to platform (TPM) which authenticates platform to the network.

3.3 Digital Certificates

A digital certificate is the electronic version of a personal identification card, such as a driver's license or passport. The process for validating a digital certificate is similar to the process used to issue a physical ID card. A *certification authority* validates information about software developers and then issues them digital certificates to be used as their personal identification. The digital certificate contains information about the person to whom the certificate was issued, as well as information about the certifying authority that issued it. Additionally, some certifying authorities may themselves be certified by a hierarchy of one or more certifying authorities, and this information is included as part of the certificate. When a digital certificate is used to sign programs, ActiveX controls, and documents, this ID information is stored with the signed item in a secure and verifiable form so that it can be displayed to a user to establish a trust relationship.

A digital certificate usually consists of identifier field, public key field, serial number (of certificate), activation and expiration date, and signature field. X.509 defines a standard format.

Digital certificates use a technology called *public-key cryptography* to sign software publications and to verify the integrity of the certificate itself. Public-key cryptography uses a matched pair of encryption and decryption keys called a *public key* and a *private key*. The public-key cryptography algorithms perform a one-way unscrambling of the data they are applied to, so that data that is encrypted with the private key can only be decrypted by the corresponding public key. Additionally, each key uses a sufficiently large value to make it computationally infeasible to derive a private key from its corresponding public key. That means that someone having your public key can certainly decrypt data generated with your private key, but they cannot reverse engineer your private key in order to masquerade data purporting to come from you. For this reason, a public key can be made widely available without posing a risk to security.

To further reduce the possibility that someone will derive a private key from its public key, the certifying authority time-stamps the key pair so that they must be replaced periodically, and provides an additional mechanism to assure that a signature was applied before the certificate expired. Any signature applied during the active lifetime of the digital certificate will remain valid for an unlimited time (unless the signed item is tampered with or the signature is removed). Any signature applied after the digital certificate expires is invalid and can easily be detected.

3.4 Firewall

As the front line of defense for many companies, firewalls sit between the corporate intranet and the Internet, and manage public access to the network’s resources and data. They can be used within the enterprise to provide an additional layer of security for your most sensitive systems.

A firewall provides access control and prevents unauthorized access to or from private networks. As depicted in Figure 10, all messages entering or leaving firewall protected networks pass through the firewall, which examines each message and blocks messages that do not meet the specified security criteria. This is one of the fundamental components of a secure network. Firewalls come in various flavors; two of most interest here are software firewall solutions installed on the local PC and hardware based firewalls designed to protect the enterprise connection.

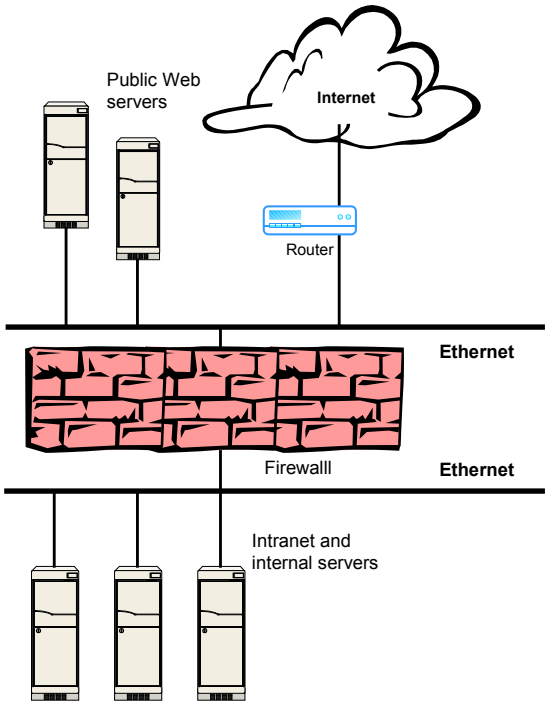


Figure 10: Firewall

Keeping intruders from reaching through an outside connection into any PC in the first place is clearly the best solution. That's why most enterprises use a real hardware-based firewall, where the LAN connects to the outside world. Furthermore, many small office and home office installations have firewall functions built into the external routers and other Internet-connection sharing devices they may employ.

When it comes to information security, it is risky to depend on a single line of defense. First, a firewall can fail; no piece of hardware or software is perfect, and as can be imagined, all have at least one weakness that can become an access tunnel to a hacker. Second, a conventional firewall may do nothing at all to protect against attacks that originate on the "safe" side of the connection or that attempt their dirty work via the usually lightly guarded outbound Internet link. As shown in Figure 2 of Section 2 in this document, hacking from inside the corporation happens. These attacks can result from hacking by employees “testing for security holes” (across the local network) or from Trojans, worms, and "phone-home" spyware installed on systems found on the “safe side” of the network.

A good desktop firewall, implemented through software installed on the PC, can help. First, it can serve as a primary firewall if the main firewall protection fails for any reason. Second, a desktop firewall can help thwart hacking from the “friendly side” of the LAN connection and also block attempts by locally installed software to co-opt or hijack the Internet connection, preventing back-door or phone-home activities.

A Packet Filtering hardware-based firewall (WAN to LAN) in its simplest form, is a firewall that serves as a packet filter, just as its name implies. Packets enter the system from the WAN (the first 10/100-Mbps Ethernet interface connected to the WAN router), are classified, and are then either passed to the LAN (the second 10/100-Mbps Ethernet interface) or the packet is logged/dropped. Packet headers are inspected or evaluated based upon policy software. This

policy is maintained in a series of tables or a simple database for applications that may need greater levels of inspection. Filters may be established based on any element within a packet header. Filters based on source IP addresses and TCP ports are common examples. Filters are also often established for Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) packets to maintain desired levels of monitoring and security across the network. This TCP/IP packet diagram identifies various elements of the TCP, IP, and Ethernet header that are important to the establishment of firewall policy algorithms.

Firewall functions can include:

- The firewall examines each packet entering or leaving the network and accepts or rejects it based on a predetermined list of criteria.
- The firewall provides an applications gateway that can apply security mechanisms to applications such a FTP or Telnet servers.
- Circuit-level gateways apply security when a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) connection is established.
- A proxy server intercepts all messages entering and leaving the network, while hiding the true network address.

Current generation firewalls must obtain, store, retrieve, and manipulate information derived from many communication layers and other applications. For this to occur, packet streams that contain information derived from previous activity must be monitored. This state information must be tracked, analyzed, and acted upon.

Types of state information include:

- Basic Packet Information: Information from all seven layers in the packet
- Derived Information: The state derived from previous communications
- Application-Derived: The state information derived from other applications
- Information Manipulation: The evaluation of flexible expressions based on all the above factors

Proxy Firewall (LAN to WAN)

Often referred to as proxy services, a Proxy Firewall application takes user requests to the WAN (10/100-Mbps Ethernet interface connected to the WAN router) and forwards them as appropriate according to a security policy. The proxy application evaluates the request (packet header inspection) from the LAN user and either approves the request, contacts the destination site/service and replaces the source IP address with its own, or denies the request (such as a denial of streaming video services).

Virtual Private Network

A VPN is essentially a secure tunnel over a shared network infrastructure. This shared infrastructure is usually the Internet, but a VPN tunnel can be established over most any communications link. In this tunnel, the data being transferred is encrypted and then encapsulated within an IP packet to prevent packets unraveled and potentially visible to unauthorized eyes.

Like routers, firewalls must process all IP traffic, passing information based on filters that are defined for the firewall. Firewall VPNs are best used when frequent reconfiguration is not required.

3.5 VPN (Virtual Private Network)

The very nature of notebook users presupposes that the PC will be used in a variety of locations, not necessarily fixed in one location such as the office, and that the user needs access back to the resources provided by the corporate network. Gaining this access traditionally has meant making a connecting using a dial-up modem and transmitting data across a relatively insecure (and *slow*) connection. Use of a secure dial up link has not been a viable option for the nomadic or roaming notebook user because of the increased security risk. VPN (virtual private network) provides a method to utilize *any* communications link to securely connect to the corporate network. For example, if a user can access the Internet through a high speed broadband data connection in a hotel room or coffee shop, a VPN can provide the secure tunnel to keep that communications link safe.

The basic architecture for all remote access is a connection from a remote site through a network to a central or other branch site. In the past, organizations that required a secure network were forced to lease public telecommunication lines or use frame relay circuits. This may be a safe solution, but it is also expensive, relatively inflexible, difficult to manage, and does not easily support remote users.

The strength of a VPN is its ability to transmit information securely and reliably over any existing unsecured public telecommunication infrastructure. A VPN is a 'virtual network' since connections are established only on an as-needed basis. The transmitted information is encrypted and tunneled point-to-point over a packet-switched unsecure network. At the receiving end, the information is decrypted, filtered if necessary, and checked for integrity. A VPN provides network users with an inexpensive, safe and scalable security solution. A VPN is a communications network built for the private use of the enterprise over shared public facilities (Internet). There are two primary applications covered by this definition: single-user remote access and site-to-site access. The beauty of either VPN application is that it goes through the Internet, creating a virtual "tunnel" that protects sensitive corporate data.

A VPN-based remote access connection begins with the single user dialing into a local POP via a direct dial link or an established broadband connection. Once connected and authenticated with the local POP, the single user launches the VPN client software, using a combination of encryption and authentication technologies to establish a secure tunnel over the Internet to a VPN Gateway running at the edge of the corporate environment. Once this connection has been established, the user can access all company resources via the Internet in a more cost-effective manner than with a traditional direct dial connection. All data transmitted and received by the single user is encrypted using various methods, ensuring confidentiality of corporate information. Secure data transmission over the public network is ensured.

The second application, site-to-site based VPN, is essentially a private network utilizing public facilities. Site-to-site based VPN provides levels of security, privacy, and manageability that are comparable to traditional site-to-site networks based upon costly private leased-line (T1/E1 or Frame Relay) connectivity (WAN). VPN does not require end-to-end leased lines and therefore

any associated costs will be lower. The VPN-enabled devices only require access to the Internet via an ISP.

To summarize, leased lines provide inherent benefits such as security, reliable access to bandwidth, and guaranteed quality levels. On the downside, however, leased lines can be very expensive. Since a company pays for the dedicated line(s) whether or not the bandwidth is used, the operating costs tend to be high. In addition to the direct lease costs, the company must buy, configure, and maintain the terminal equipment connecting the end-to-end sites. In addition, if remote users are expected to connect to this WAN, RAS equipment must be purchased and maintained, thereby increasing the overall WAN costs. As an alternative to the costly leased line option a VPN site-to-site configuration would eliminate the need for dedicated leased lines while providing a secure and effective Intranet solution.

Figure 11 below illustrates a fully integrated traditional remote access and Virtual Private Networking solution supporting single-user and site-to-site scenarios.

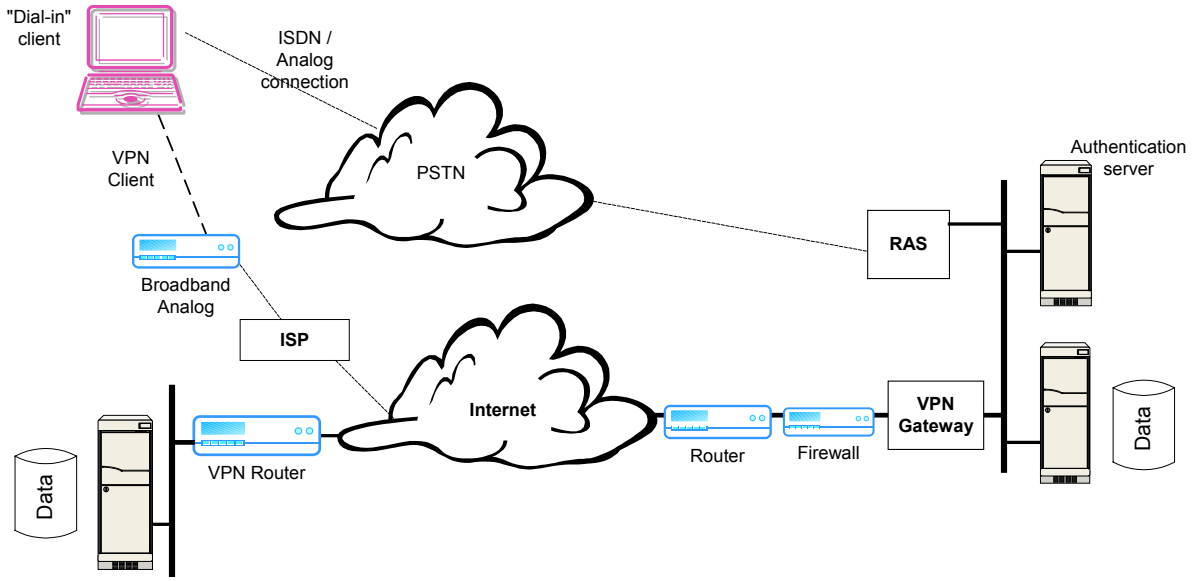


Figure 11: Remote VPN Access

In today's remote access environment, VPNs and direct dial are not necessarily mutually exclusive. In fact, leveraging the advantages of direct dial with the lower costs of VPN usually provides the most cost-effective remote access solution. While VPN is most effective for long-distance applications, direct dial is an effective means for local access or backup. In order to optimize the remote access solution, an IS manager should consider integrating VPN connectivity with traditional direct dial access. Virtual Private Networking provides the following advantages:

- **Cost:** The major cost in a direct dial solution is the time and distance-based charge to use the telephone system. VPN can greatly reduce long distance charges. However, if most of the users are local to the corporate LAN, long distance cost savings will not apply. Therefore, when designing a remote access solution, the geographic location of the users will determine the optimum solution. In most cases, this will be a combination of direct dial and VPN. Note, if this is a new remote access network, depending on applications

and corporate policies, direct dial capabilities can be subscribed from an ISP, possibly reducing overhead costs.

- **Performance:** The overall performance in a traditional direct dial connection is limited by the "last mile" infrastructure and the technologies used at the client site (i.e., 56Kbps modem over a voice circuit). From a performance point of view, one of the major advantages of VPN is the ability to use the newer broadband technologies to access the Internet. These higher speeds reduce latency introduced in the "last mile" over traditional telephone lines and can generate significant time and cost savings to the organization.
- **Authentication:** With VPN, traffic arrives from the "unsecure" Internet and therefore it is especially important to authenticate the connection when establishing the VPN tunnel. Administrators can choose from a variety of authentication techniques from basic usernames and passwords to the more secure token and X.509 digital certificate option. Another very popular option is to use RADIUS authentication software. RADIUS authentication can be easily integrated into a corporation's current network by configuring the RADIUS server to authenticate VPN and direct dial users by proxying to a Windows NT* or Novell* NetWare* Directory Services (NDS) server. This option has the advantage of simplicity and ease of deployment. The secure token and digital certificate option provides enhanced security over traditional username and password schemes since tokens and certificates rely on third-party security software and thus are less susceptible to password hacking. Whichever method is implemented, the security manager should balance the need for data protection with the need for ease of use.
- **Data Integrity:** Data transmitted through the Internet is susceptible to corruption and manipulation by unauthorized users. This potential security breach should be a concern for every corporate IT Security manager. VPN solutions, unlike traditional dial networks, use cryptographic techniques, ensuring data cannot be manipulated by a hacker while in transit. Once a VPN tunnel has been established between the client and the corporate VPN gateway, all "payload" data is encrypted as it leaves the transmitting device and is decrypted on the other end by the receiving device. Encryption is the process of running the users' data through an encryption algorithm and producing a "ciphered" text. Any device maintaining the same algorithm and "cipher key" can then decode this "ciphered" data. The result: all transmitted data is unreadable except by authorized end devices.

As with any networking technology there are issues that could affect the data transfer rate within a VPN-installed network for the mobile user. A few factors limiting the overall VPN performance include the "last mile" technology, Internet latency and encryption overhead. Any of these considerations can be effectively managed to the point where they have little to no effect on a corporate VPN network. If they can be identified, any issue can be mitigated.

By reducing the cost of retrieving information from the Internet, an organization can significantly increase productivity and boost company value. This is especially true for organizations that provide employees with notebook computers where work can be done from the traditional office, at home, or from any location almost anytime.

VPNs provide an excellent method of securing any type of wireless connection regardless of its physical relationship to the enterprise. For example, 802.11 networks deployed within a large building of a corporation are vulnerable to security breaches because of the very nature of the wireless connection. Adding VPN to such wireless network access is a means to ensure

complete confidence that data is protected as it travels across radio links. Hackers sitting in the parking lot may be able to access such wireless traffic, but if it is encrypted using a VPN tunnel, those hackers will not be able to decrypt that data. Section 4.1.2.6 discusses the use of future implementations 802.11i as a provision to secure a wireless network within the enterprise, but VPN is recommended to provide a safe link for connections to/from outside the corporate enterprise.

Specific use of security algorithms and how the VPN takes advantage of any type of hardware security device for encryption and authentication takes a variety of directions depending on the VPN vendor. Some VPN solutions take advantage of standards based software interfaces so that the strength of the encryption and authentication can be tailored to whatever solution is needed by the corporate enterprise. On the other extreme, some VPN implementations use proprietary encryption protocols and are tied to specific authentication mechanisms which may work for some customers, but are not flexible to meet the needs of others.

In summary, Virtual Private Networking (VPN) makes it possible for users on an un-trusted public network, such as the Internet, or using any type of wireless network within the enterprise, to connect to a private network in an easy and secure manner. VPN data is encrypted and encapsulated inside a tunnel as it travels through the connection. For business networks, a VPN solution for wireless access is currently the most suitable addition to WEP and MAC address filtering. With a VPN solution, various industry-standard security mechanisms are employed to safeguard data and ensure that only authorized users can access the network. VPNs support a variety of user authentication methods, such as RADIUS, SecureID and digital certificates. These standards based methods allow easy integration into existing network infrastructures.

3.6 Virus Protection

Viruses are self-replicating, malicious programs, often carried in email attachments, that can spread rapidly across a network, deleting and modifying files and causing other damage. Both email servers and client systems need virus protection to keep such software from causing problems both internally as well as from replicating and causing problems elsewhere. Rogue software is a virus classification that infects ActiveX* controls or Java* applets, or can be downloaded as ActiveX* or Java* applets entirely.

A variety of security threats pose problems to the user and corporate infrastructure. These of course are magnified in a wireless environment where the user can theoretically maintain constant connection to the Internet and email. Virus software is one of the leading problems plaguing the computing industry that is propagated through email and Internet connections. It seems that individuals create virus problems either intentionally malicious or “just because they can”. Protection against such virus threats in their many permutations can be provided on a personal computer by installing the most advanced and reliable virus protection available that is kept up-to-date with detection, prevention, and eradication methods for the latest problems floating the ether.

Virus protection software can scan and clean e-mail messages on a real-time basis before they ever reach your computer. By configuring the virus scan software correctly, it can repair common virus infections automatically, without interrupting your work. Not only must every computer be capable of detecting a virus to avoid problems, but also eradicating the virus so that others don’t experience problems as the virus may replicate to other machines.

Anti-virus software should be used to protect against software embedded in e-mail, which can perform tasks such as stealing data, erasing files, reformatting hard drives or writing messages to a computer's display. In addition, anti-virus tools should be installed both on a gateway machine that inspects all incoming and outgoing e-mail as well as on each individual workstation to provide adequate coverage against this threat.

There are three technical strategies for identifying, capturing, and controlling virus software.

Signature Scanning. Signature scanning refers to identifying unwanted code. For a virus, this means scanning every application load module for indications of virus infection. Each virus has its own signature or fingerprint that results from the way it links itself into the application and the replication code that is attached. New viruses are continually being developed, so signature files must be continuously updated that reflect the unique identifiers of every virus found by the security vendor. The signature file that is used for this scanning process can be stored on servers if the security administrator wants to scan only when end users are connected to the network. Users not connected to the network need the signature files on their local hard drives. Continuous update of the signature files is difficult in these circumstances. Network login scripts should force signature updates onto every computer. Signature scanning can also identify rogue applications. Scanning signatures derived from the application code in a manner similar to virus signatures is the most reliable method. Other approaches include using embedded digital signatures (if they are present) and "by name" identification, in which rogue applications are identified by some embedded name. A virus can also infect a Java applet or ActiveX component, so the security administrator must do normal virus signature scanning in addition to rogue identification.

Heuristic Scanning. Heuristic scanning attempts to determine evil intent by predicting what actions will take place when the application executes. This identification strategy is common to containing both viruses and rogues. The security software simulates the execution of the software and identifies probable attempted unauthorized accesses. This is useful as an additional method of finding offending code for which no signature is available. For heuristic scanning to be both effective and economical (in terms of system overhead), the scanning software must make assumptions regarding both appropriate security policy and probable application strategies to bypass the policies. It does not verify every possible execution path in the program.

Effective Authorization and Access Control. A simplistic solution for identifying, capturing, and controlling virus and rogue software is to do nothing about the virus and rogue problem. Security managers, can simply select strong, secure operating systems and ensure these systems are enforcing the enterprise's security policy. Sound like a bad solution? Unluckily, this solution eliminates the use of most common PC operating systems, and it may thus prove infeasible.

A complete solution, given the variety of threats and weaknesses in current computing environments, requires a multi-tiered architecture for virus and rogue protection. The PC should detect unauthorized behavior and stop it. The rogue-control software should notify an enterprise console or operations site of the attempted violation.

Firewalls should block further passage of that module to prevent infection at PCs that are less well protected. A central tool for security administration should set the policies that are enforced at every PC. No system for preventing viruses or rogues is effective unless the enterprise has a reasonable level of configuration management over PCs. The best signature files in the world

are useless if they are not installed where they are needed. Inadequate configuration management currently is the most common cause of virus infection.

Besides the preventative actions for virus prevention, detection, and eradication, there are considerations for keeping viruses from causing problems.

1. Viruses are spread through data transmitted from one machine to another -- In most cases, viruses are spread through an electronic network connection which takes the predominant form of the Internet. Emails sent can have “mysterious attachments” with malicious nature of infinite varieties and intents. The objective should be to secure network traffic not only from the outside of the enterprise, but also from malicious or innocent-yet-harmful threats spread from within the enterprise.
2. Not every virus alert is legitimate -- If you've seen or read about a new virus via a reputable news source or publication, it is probably not a hoax. However, if you receive an e-mail, even from someone you know and/or trust, regarding a new virus alert that asks you to pass it along, you should validate the alert before doing anything! This is a common trick used by virus creators to spread the infection. Many virus alerts have been spread via email across the Internet claiming a threatening software on your PC with instructions to delete a file – and it turns out that the file is a legitimate file that poses no threat. Instead of forwarding a virus alert e-mail to your address list or proceeding to “clean up” the virus, first confirm whether or not the virus alert is real by contacting either your anti-virus vendor or corporate IT department. If you are able to confirm that the virus threat is real, the next course of action is to fix it.
3. Determine if a virus infection has attacked -- Unless your computer has anti-virus software or your corporate IT infrastructure periodically scans your PC via a network connection, it is difficult to determine if a virus has infected your PC. In many cases, a virus can slow your computer's processor or trigger other unusual behavior; however, these symptoms can also be caused by a number of unrelated reasons.

   Either the user or the corporate IT support team must ensure that every PC has the latest virus definitions running. This can be done by regularly visiting your anti-virus software vendor's Web site to download them, or by running scheduled updates to anti-virus software. Without these regular updates, it is impossible to detect and prevent virus attacks.
4. Virus Removal -- As virus detection software identifies that a virus exists, that anti-virus software should be able to remove the virus before it proceeds to cause damage. It may be necessary to get the latest updates from the anti-virus software vendor's Web site to download the latest definitions or updates that will fix or remove the virus. In some cases, it may be necessary to follow the steps provided to manually remove viral code within the PC.

   In most cases, the latest virus definitions from your anti-virus software vendor will completely remove the virus. However, many times a Trojan horse is spread like a virus or could be spread with a virus, but may not immediately show symptoms. If you notice your computer or Internet connection running without your using it, or if your computer settings change, you should go to your anti-virus software vendor's

Web site to install the latest definitions or scan your machine to detect the presence of any Trojan horses.

5. Virus Protection -- There is no single, fail-safe solution that will protect your computer or files from infection. The best strategy against any security breach is a well-informed and proactive defense.

The most important actions to take include:

- **Install anti-virus software and keep it current.** There are many good vendors who provide solid virus detection, protection, and eradication and they stay on top of the latest virus threats to provide solutions when needed.
- **Acquire regular operating system updates.** These updates may solve some problems or anomalies where virus can take advantage to create problems. In the case of Microsoft* Windows*, "Windows Update" can be used to scan and update the Windows* operating system with the latest free software patches, including those for Microsoft Internet Explorer and Microsoft Outlook Express.
- **Install updated application software.** The same thing is true for applications used regularly: keep the software up to date by acquiring current releases from the respective vendors. Many application vendors provide a mechanism to update software from their Internet web sites. Having up-to-date application software can help prevent possible security holes that virus software often uses as a point of attack.
- **Personal firewall.** To help prevent virus software from creeping onto your system without your knowledge, it may also help to install a firewall, especially if you use a high-speed Internet connection. Firewalls can take the form of either hardware or software, and are discussed in another section of this document.
- **Use caution when traveling the Internet.** Be cautious about visiting unknown or untrusted Web sites. Untrusted or disreputable Web sites can transmit a virus directly into your computer without you realizing it. Staying on the main routes of the information highway will help keep you safer.
- **Use judgment when opening email.** Don't open e-mail attachments from anyone you don't know—and be wary of those from people you do. Viruses can spread by mailing themselves to contacts in an infected computer's address book. If you have any doubts about the safety of an attachment, check with the source before opening it. Virus detection software configurations should be set to analyze not only the email, but also attachments of email that you receive.

By using discretion, keeping your anti-virus software up-to-date, policies established and properly configured, and erring on the side of caution, you can help correct and protect the health of your computer system and systems within your enterprise. Simple steps of prevention are often easier to apply than solving problems generated by viruses after they attack.

3.7 General Security Infrastructure Recommendations

Client systems play an important role in enterprise information security. To maximize security, client systems should run a variety of information security technologies:

- Anti-virus software with continuous scanning, so the system is safeguarded against viruses lurking in e-mail attachments, web downloads, or even screen savers.
- Encryption, to protect files stored on the hard drive and sensitive information sent as email attachments.
- Public key cryptography, such as the Public Key Infrastructure (PKI), are essential services for providing strong authentication, access control and data integrity.
- Personal firewalls protect client systems from attacks while also limiting users' ability to gain unauthorized access to network resources.

These technologies often run transparently in the background, adding to the demands on the system while the user is trying to get work done. And they can consume enough processing cycles to have a noticeable impact on the system's responsiveness. Use of specialized hardware security devices such as a smart card or TPM can reduce the workload needed to keep the system safe. High performance Intel processors provide the extra computing headroom to run these background tasks without noticeably slowing the system down[3].

4 Wireless Technologies

Increasingly, IT managers are realizing the benefits of wireless connectivity, but anywhere, anytime access comes at a price: these wireless networks can be difficult to administer and secure. For SOHO notebook customers, the use of wireless LANs and other wireless technologies helps reduce cabling problems, improves data access regardless of location, and increases productivity. Regardless of whether the notebook user is part of a large corporation or a one-man-show, mobile workers demand wireless connections for ease of use and increased productivity which can bring numerous challenges.

Wireless technologies, such as 802.11b, Bluetooth*, Wide Area Networking (WAN), are continuing to gain acceptance as most notebook manufacturers include integration of some of these protocols as options on notebooks, and some vendors have begun to integrate them as standard features. Standardization of wireless computing protocols is expected to spur increased enterprise demand. Wireless connectivity further expands the "work anywhere" mantra of modern business and is expected to add to productivity gains by mobile workers. Most notebook PC vendors now support at least one wireless protocol (in some cases more). The wireless capabilities of notebook computers continues to increase in business and home use many desktops are replaced with new wireless capable notebooks.

4.1 802.11 Wireless LAN

A Wireless Local-Area Network (WLAN) uses radio frequency technology to transmit and receive data over the air, providing all the features and benefits of traditional LANs but without

[3] Industry-standard benchmarks show that when a PC powered by an Intel® Pentium® 4 processor at 2 GHz ran the BAPCo* SYSmark2001* benchmark with the Microsoft* Encrypting File System's 168-bit encryption activated, its performance on common productivity tasks slowed enough to put it at about the same level as a Pentium 4 processor at 1.70 GHz.

the limitations of a cable. Most WLANs today use the 2.4Ghz frequency band (802.11b) with next generation 802.11a utilizing the 5Ghz band.

The IEEE 802.11 standard has emerged as the predominant standard for WLANs. 802.11b (sometimes referred to as "WiFi") supports any existing LAN application , network operating system, or protocol, including TCP/IP, as easily as if they were run over wired Ethernet.

Wireless networks are now becoming widely deployed, and manufacturers have accelerated the deployment of low-cost, interoperable wireless LAN products. Today's 802.11 wireless technology promises to open up exciting new possibilities. However, as WLANs become more numerous and widespread, more robust security solutions are required.

In particular, recent demonstrations of the vulnerability of the RC4 cipher, which forms the basis for Wired Equivalency Privacy (WEP) encryption, make it clear that WEP protection alone is inadequate. A robust and scaleable security solution for wireless networking must address all the data security concerns.

4.1.1 802.11 Security Concerns and Threats

The 802.11 standard failed to deliver any workable security provisions acceptable to those who recognize the value of data security in this brave, new wireless world. In the early days, people thought of 802.11's ESSID (extended service set identifier), a string that was defined for each access point, as a wireless password. But implementers soon discovered that the access points routinely broadcast these "wireless passwords" over the LAN. Even when broadcasting was disabled, the strings could be extracted in clear text form out of the management frames passed by wireless clients and access points. Today, ESSIDs are often detected automatically by WLAN clients, letting users connect to wireless networks transparently, provided no other security points exist.

In many cases, security deployment of 802.11 wireless LANs in home or business is expected to be provided simply by physical distance of the wireless LAN from any possible threat of "radio wave eavesdropping". The range for 802.11 is expected to cover only a distance of up to ~100feet. Some implementations assume that since there is no way for a hacker to get within 100 feet of the 802.11 appliances, there is no way for the hacker to listen to 802.11 radio transmissions. In some respects, this is true – standard antennas for 802.11 only work within that relatively short range. However, it is quite easy to acquire antennas for 802.11 that can sniff 802.11 radio traffic up to ½ mile away. Hence, if someone wants to listen to 802.11 radio traffic, physical proximity should not be considered any sort of security provision.

Since the 802.11 standard doesn't provide an authentication framework, sites sometimes implement MAC (Media Access Control) address restrictions to control access to the network. However, this approach causes an administrative burden, is vulnerable to address spoofing, and it ties access to the device (which can be stolen) rather than to the user.

WEP (Wired Equivalency Privacy) was defined within the 802.11 standard as a security feature. It was intended to provide privacy equivalent to the privacy available a wired LAN. In reality, WEP falls short of that goal. Noted security experts Scott Fluhrer, Itsik Mantin, and Adi Shamir pointed out security holes in WEPs design in an article from 2001 (see "Your 802.11 Wireless Network Has No Clothes", http://www.cs.umd.edu/~waa/wireless.pdf). Even if these experts hadn't exposed the weaknesses in WEP's encryption system, the static shared-key architecture

has little appeal for enterprise IT professionals. As such, there is a need for privacy based on dynamic session keys that are distributed after a robust authentication to keep hackers at bay.

It is almost impossible to eliminate wayward hackers who are constantly searching for new ways to attack wireless LAN connections. Today's wireless LANs are especially inviting because the built-in security available to them (WEP) is not the robust security solution today's users need and demand which makes it an easy target for hackers. For instance, the default configuration in most wireless LAN networking equipment has WEP encryption turned *off*, and many installations never adjust the configuration to turn it *on*. If current implementations of WEP wireless networks aren't activated, all data, including passwords, is sent as unencrypted, in-the-clear text. Even if WEP is activated, hackers can fairly easily obtain the encryption keys the protocol uses to scramble and unscramble data by capturing the data flows on a wireless LAN -- a process that can take as little as 15 minutes using a power of a notebook computer. Other security features built into wireless LANs include nothing more than the most rudimentary access-control and user-authentication mechanisms that attackers can easily trick into thinking they're legitimate users.

Because of WEP's security limitations and the fact that wireless LAN data traffic is easily sniffed regardless of physical barriers, a wireless network without additional security mechanisms leaves the door open for a hacker to do all the evil things known to plague wired LANs and Internet servers: exploit software and operating-system vulnerabilities, plant a back door or other eavesdropping software into the network, or deface Web pages.

4.1.2 802.11 Security Primitives

802.11 wireless LANs provide a number of security primitives, each with different intent, different strengths and weakness. In order to provide a safe connection with 802.11, a combination of properly configured primitives must be used.

4.1.2.1 Service Set Identifier (SSID)

The SSID allows a WLAN to be segmented into multiple networks, each with a different identifier. For example, a building might be segmented into multiple networks by floor or department. Each of these networks is assigned a unique identifier, which is programmed into one or more APs – each network can consist of multiple APs. To access any of these networks, a client computer must be configured with the corresponding SSID for that network. Thus, the SSID acts as a simple password, providing a measure of security. A weakness is that the SSID is widely known and shared. Many deployments do not change the default SSID as it shipped from the manufacturer, and therefore it is not difficult to get access to those unconfigured WLANs simply by guessing the SSID.

4.1.2.2 Media Access Control

To increase security, each AP can be configured with a list of MAC addresses associated with the client computer that are allowed access to the AP. If a client's MAC address is not on the list, the AP will deny access. This method provides good security but is only suited to small networks. The labor intensive work of entering MAC addresses and maintaining up-to-date lists on all of the AP devices obviously limits the scalability of this approach.

4.1.2.3 Wired Equivalency Privacy (WEP)

To minimize the risk of RF interception by someone nearby – for example, someone sitting in the parking lot or a hacker using a high-gain antennae from a long distance – WEP is specified for encryption and authentication between clients and APs according to the 802.11 standard. WEP security is based on an encryption algorithm called RC4* from RSA Data Systems*. The encryption algorithm is generated based on a key (a number sequence) entered and controlled by the user. All clients and APs are configured with the same key to encrypt and decrypt transmissions. WEP keys vary from 40 to 128 bits in length.

An AP can be set up to provide encryption-only protection in open-system mode, or to add authentication in shared-key mode. MAC address filtering is often used together with this encryption. WEP security is best suited for small networks, as there is no key management protocol. As a result, keys must be manually entered into every client. This is a huge management task, especially since the keys should be changed regularly to provide an extra measure of security.

Many papers and articles have been written describing the vulnerability of the RC4 cipher used in WEP. Breaking the encryption used in RC4 is done by attacking weaknesses in the key-scheduling algorithm of RC4 to obtain the network key. With the right software that is readily available from the Internet (such as AirSnort or WEPCrack), anyone with a laptop with a WiFi network card can gain access to a "WEP protected" WLAN in less than 15 minutes. WEP protection alone is clearly not enough.

4.1.2.4 802.1X

IEEE 802.1X is a standard for port-based network access control that provides authenticated network access to 802.11 wireless networks and wired Ethernet networks. 801.1X is not an authentication algorithm itself. Rather, it translates messages from an authentication algorithm into the appropriate frame formats of the LAN access types, below. The LAN type pertinent to this discussion is 802.11, but 802.1X can also be used as the authentication method for other 802-based LANs, including 802.3 Ethernet or 802.5 Token Ring. Port-based network access control uses the physical characteristics of a switched local area network (LAN) infrastructure to authenticate devices that are attached to a LAN port and to prevent access to that port in cases where the authentication process fails.

During a port-based network access control interaction, a LAN port adopts one of two roles: *authenticator* or *supplicant*. In the role of authenticator, a LAN port enforces authentication before it allows user access to the services that can be accessed through that port. In the role of supplicant, a LAN port requests access to the services that can be accessed through the authenticator's port. An *authentication server*, such as such as a Remote Authentication Dial-In User Service (RADIUS) server, which can either be a separate entity or co-located with the authenticator, checks the supplicant's credentials on behalf of the authenticator. The authentication server then responds to the authenticator, indicating whether the supplicant is authorized to access the authenticator's services.

The authenticator's port-based network access control defines two logical access points to the LAN, through one physical LAN port. The first logical access point, the *uncontrolled port*, allows data exchange between the authenticator and other computers on the LAN, regardless of

the computer's authorization state. The second logical access point, the *controlled port*, allows data exchange between an authenticated LAN user and the authenticator.

802.1X supports two subtypes of authentication services: *open system* and *shared key*. *Open system* is a default null authentication algorithm that involves a two-step process consisting of an identity assertion and request for authentication followed by an authentication result. *Shared key* authentication assumes that each wireless station has received a secret shared key over a secure channel that is independent from the 802.1c wireless network communications channel.

802.1X does not require that the same WEP keys be used by all wireless stations. The WEP algorithm defines the use of 40-bit secret keys for authentication and encryption. 802.1X allows a station to maintain two sets of shared keys: a per-station unicast session key and a multicast/global key. Current 802.1c implementations primarily support shared multicast/global keys but are expected to support per-station unicast session keys in the near future.

An extension to the basic 802.1X protocol is required to allow a wireless access point to securely identify traffic of a particular client. This is done by passing an authentication key to the client as well as the wireless access point as part of the authentication procedure. Only authenticated clients may know the authentication key, which encrypts all packets sent by a client.

Without a valid authentication key, an authenticator inhibits all network traffic. When a wireless supplicant comes in range of a wireless authenticator, the following steps occur:

1. The wireless authenticator issues a challenge to the wireless supplicant.
2. Upon receiving the challenge from the authenticator, the supplicant sends its identity to the authenticator.
3. The authenticator forwards the identity of the supplicant to the RADIUS server to initiate authentication services.
4. The RADIUS server then requests the credentials for the supplicant, specifying the type of credentials required in order to confirm identity.
5. Requests passing between the supplicant and the RADIUS server pass through the uncontrolled port on the authenticator, because the supplicant cannot directly reach the RADIUS server. The authenticator does not allow communication through the controlled port as the supplicant does not possess an authentication key.
6. The supplicant sends the credentials to the RADIUS server.
7. Upon validating the credentials, the RADIUS server transmits an authentication key to the authenticator. The authentication key is encrypted so that only the authenticator can access it.
8. The authenticator uses the authentication key received from the RADIUS server to securely transmit a per-supplicant unicast session key and a multicast/global authentication key to the supplicant.

In order to encrypt the global authentication key, the Extensible Authentication Protocol (EAP) authentication method used for wireless must be capable of generating an encryption key as part of the authentication process.

Transport Level Security (TLS) provides for mutual authentication, integrity-protected cipher suite negotiation and key exchange between the two endpoints. Therefore, EAP and TLS will be used to provide for the TLS mechanisms within EAP.

Support for 802.1X is provided in Windows XP* Professional. It is recommended that this be configured for use with Intel network products to improve user authentication for 802.11 wireless networks.

4.1.2.5 Virtual Private Network (VPN)

As described in Section 3.5 of this document, VPN is a technology that makes it possible for users on an un-trusted network to connect to a private network in an easy yet secure manner. VPNs are already widely used for remote access and intranet connections including 802.11 wireless connections. They employ various industry standard security mechanisms to safeguard data and ensure that only authorized users can access the network. For business networks, a VPN solution for wireless access is currently the most suitable solution to the weakness of other existing 802.11 security measures.

IPSec (Internet Protocol Security) as defined by the IEEE, is the most widely used mechanism for securing VPN traffic. IPSec can use various security algorithms including DES, 3DES and other bulk algorithms for encrypting data, keyed hash algorithms (HMAC, MD5, SHA) for authenticating packets, and digital certificates for validating public keys. VPNs also support a variety of user authentication methods such as RADIUS, SecureID, and digital certificates which may be stored in a hardware security device (smart card, USB security token, or TPM). These standards based methods allow for easy integration into existing network infrastructures.

The IPSec protocol includes three principal security elements:

1. Authentication Header (AH) – The AH provides authentication and integrity by adding authentication information to the IP datagram. This ensures that the data will not be available to an unauthorized station and will not be altered en route.
2. Encapsulation Security Payload (ESP) – The ESP provides confidentiality. It can also provide integrity and authentication, depending on the algorithm used. With the ESP in use, part of the ESP header itself and all data contained in the datagram is encrypted. Tunnel or transport modes are available, with tunnel mode being the choice for remote access.
3. Internet Key Exchange (IKE) – This is the key management protocol that is used to negotiate the cryptographic algorithm choices to be employed by the AH and ESP. The mechanisms used in IKE provide for an extremely scaleable solution. The Diffie-Hellman algorithm also plays an important role in ensuring that the keys are exchanged securely.

Additional information for VPNs is found in Section 3.5 of this document.

4.1.2.6 802.11TGi

The IEEE 802.11i Technical Working Group is actively defining ways to improve 802.11 security, particularly in how it handles key generation for coding data that's in transit. In addition, the group is considering other improvements designed to protect wireless networks

against common attack methods, including Initialization Vector collision, replay attacks, and forged packets. The current encryption in WEP, RC4 may be replaced by Advanced Encryption Standard which should provide better encryption.

A draft of IEEE's 802.11i spec to beef up security on 802.11 wireless networks was finalized January 21, 2002 and is now circulating within the engineering community for editing and subsequent approval. The security algorithm included in that 802.11i draft, called Temporal Key Integrity Protocol (TKIP) was developed with the help of some of the encryption experts that exposed WEP's vulnerabilities, TKIP, like WEP, is based on RC4 encryption -- but implemented in a different way that addresses those vulnerabilities. Among other things it generates new encryption keys for every 10 kilobytes of data transmitted.

Most, if not all, current Wi-Fi-certified products should be upgradeable to TKIP shortly after the finalization of the IEEE 802.11i specification. Those products that aren't 802.11i capable should still interoperate with existing 802.11 as well as new 802.11i products.

4.1.3 802.11 WLAN Security Recommendations and Solutions

Security threats to Wireless LAN implementations, are well-documented and factual. To safeguard information traveling across WLANs, the 802.11 standard specifies three basic methods for securing access to wireless access points, described below. Along with other industry experts, Intel considers the wired equivalent privacy (WEP) protocol built into 802.11b to be well-intentioned but flawed. Although it requires that the wireless data traffic be encrypted and that users be authenticated, the underlying structure of the encryption keys can be uncovered by unauthorized parties. It is recommended that 802.11 implementations establish a secure design and corporate policies on WLAN use, as well as using 128-bit WEP along with VPN.

For all WLAN deployments, Intel recommends the following tactical guidelines:

Establish corporate policies. These policies include security procedures for using WLANs and stipulate that only corporate IT is authorized to install WLANs that access the corporate network. They also establish a program for locating and securing WLANs that were previously deployed but not adequately secured, as well as disconnecting unauthorized and rogue access points in the wireless environment.

Evaluate physical security perimeters. Where possible, observe the grounds out to the limits of coverage and advise the security department to look out for suspicious activity. Be aware that hackers can sniff 802.11 radio traffic from long distance using an easily acquired high gain antennae. Never consider physical perimeters to be the only security mechanism used for wireless LAN.

Use security features of 802.11. Configuration of 802.11 needs to be done to improve data security, rather than assume it takes care of itself. Change the security. Do not use default service set identifier (SSID) numbers or null SSIDs. Implement media access control (MAC) address tracking to control network security, if manageable in your corporation. This recommendation is to use the built-in security features of 802.11, but don't rely solely on them.

Connect 802.11 APs to separate network segments. Implement wireless access points (APs) on switched network ports and segment onto a virtual LAN (VWAN).

Employ Wired Equivalent Privacy (WEP). WEP security is based on an encryption algorithm that is generated based on a number sequence entered and controlled by the user. All clients and

access points are configured with the same key to encrypt and decrypt transmissions. Although WEP has flaws and can be cracked fairly easily, it is still a useful additional layer of security. However, never rely solely on WEP as the only method of WLAN security.

Employ Virtual Private Networking (VPN). VPN makes it possible for users on an un-trusted network like the public Internet or a wireless carrier network to connect to a private network in an easy and secure manner. VPN employs strong authentication and encryption mechanisms and creates a tunnel between end points to protect against intrusion. Moreover, VPN is a cross-transport solution so IT groups can standardize on a VPN solution for wired and wireless security. VPN brings additional cost for deployment and management, but is worth the extra expense for enhanced security. The use of VPN for encryption with 802.1X for user authentication provides an ideal solution for secure 802.11 connectivity.

Perform multi-factor authentication. Whether it is network authentication or the addition of secondary authentication through the use of a smart card, removable security token, or even biometrics. Secondary authentication is in addition to regular network login. With a VPN solution, various industry-standard security mechanisms are employed to safeguard data and ensure that only authorized users can access the network. VPNs support a variety of user authentication methods, such as RADIUS, SecureID, smart cards, and digital certificates. Credentials and keys used in secondary authentication should be stored in hardware security devices such as smart cards or TPM to not only protect against tampering, but also provide multi-factor authentication for the connection. These standards-based methods allow easy integration into existing network infrastructures.

Implement 802.11X. 802.11X provides an additional authentication mechanism for wireless clients to connect to the corporate wireless network. Configure the wireless LAN to use 802.1X for user authentication. This can be strengthened by configuration of TLS rather than standard EAP. 802.1X is supported in Intel network products as well as within Windows XP*.

Use WLAN sniffers. Sniffers actively scan the network looking for unsecured WLAN traffic. Although users may innocently install an unsecured WLAN, their doing so can automatically breaches the security of the entire corporate network allowing a gaping hole for hackers to take advantage for ill intent. Enterprise network management should put forth effort to actively search out and disconnect rogue Wireless LAN access points in the environment.

Upgrade to 802.11i. When the IEEE finalizes and approves the 802.11i wireless standards, they will include better TKIP-based security measures, including stronger encryption and higher levels of user authentication. It is hoped that products available today may be upgradeable to 802.11i through firmware downloads, but that depends on the implementation vendor.

Keep Current. With all the solutions that are provided, so also do security threats grow and progress over time. In order to keep up with these threats, the latest and greatest patches and releases should be kept installed to provide a safe communications link for 802.11 wireless networks.

4.2 Bluetooth* Wireless Technology

Bluetooth* wireless technology was developed to provide a wireless interconnect between small mobile devices and their peripherals. The technology encompasses a simple low-cost, low-power, global radio system for integration into mobile devices. Such devices can form a quick

ad-hoc secure "piconet" and communicate among the connected devices. This technology creates many useful mobile usage models because the connections can occur while mobile devices are being carried in pockets and briefcases (therefore, there are no line-of-sight restrictions). Making all connections instantly and maintaining them even when the communicating devices aren't within line of sight, Bluetooth wireless technology enables fast, secure transmission of both voice and data.

Bluetooth radios use the globally available 2.4 GHz frequency band which ensures a universal, worldwide solution.

While the Bluetooth usage model is based on connecting devices together, it is focused on three broad categories: voice/data access points, peripheral interconnects, and Personal Area Networking (PAN).

Voice/Data Access Points
Voice/data access points is one of the key initial usage models and involves connecting a computing device to a communicating device via a secure wireless link. For example, a mobile computer equipped with Bluetooth technology could link to a mobile phone that uses Bluetooth technology to connect to the Internet to access e-mail. The mobile phone acts as a personal access point to provide a wireless data pathway to the Internet or back to a corporate enterprise network.

Peripheral Interconnects
The second category of uses, peripheral interconnects, involves connecting other devices together. Keyboards, mice, and joysticks equipped with Bluetooth technology can be used to connect back to any notebook PC equipped with the appropriate Bluetooth link. The Bluetooth link is built into the mobile computer; therefore, the cost of the peripheral device is less because an access point is not needed. For example, a Bluetooth headset used in the office could be connected to a Bluetooth access point that provides access to the office phone and multi-media functions of the mobile computer. When mobile, the same headset could be used to interface with the cellular phone (which can now remain in a briefcase or purse).

Another aspect of a short-range Bluetooth link is in the area of proximity security devices. In this case, if one device is not within range of another device, the first device will go into a high-security mode.

Personal Area Networking
Another usage model for Bluetooth technology, Personal Area Networking (PAN), focuses on the ad-hoc formation and breakdown of personal networks. Bluetooth PAN provides the ability to quickly and securely exchanging documents or sharing data by establishing a private piconet between two or more computers. The industry trend is towards using the Bluetooth 1.0 (BT 1.0) standard for wireless PANs because it defines the most efficient short-range signaling for low bit-rate applications such as printing and PDA synchronization.

4.2.1 Bluetooth Device Security

Despite reports to the contrary, security issues are not likely to derail Bluetooth as the wireless networking standard moves into the mainstream, according to recent research from Frost &

Sullivan. The Frost & Sullivan report[4] suggests that in terms of security, "the situation for Bluetooth looks much rosier than it did for Wireless LAN." Their conclusion is based on the fact that the Bluetooth Special Interest Group (SIG) has "built in some fairly robust security features" and the specifications "should provide more than enough security options and features for most users, especially if they follow good data security practices anyway." Yes, there are some security issues with Bluetooth as with all wireless communication technologies, but the support exists to overcome any problems that exist.

Bluetooth is extremely secure in that it employs several layers of data encryption and user authentication measures. Bluetooth devices use a combination of the Personal Identification Number (PIN) and a Bluetooth address to identify other Bluetooth devices. Data encryption (i.e., Bluetooth encryption based 128-bit keys) can be used to further enhance the degree of Bluetooth security. The transmission scheme, Frequency-hopping Spread Spectrum (FHSS), provides another level of security in itself. Instead of transmitting over one frequency within the 2.4 GHz band, Bluetooth radios use the FHSS technique, which allows only synchronized receivers to access the transmitted data.

FHSS is a spread spectrum modulation scheme that uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, they maintain a single logical channel. To an unintended receiver, FHSS appears as short-duration impulse noise. More simply, the data is broken down into packets and transmitted to the receiver of other devices over numerous "hop frequencies" (79 total) in a pseudo-random pattern. Only transmitters and receivers that are synchronized on the same hop frequency pattern will have access to the transmitted data. The transmitter switches hop frequencies up to 1,600 times per second (every 625 microseconds) to assure a high degree of data security.

It is difficult to even detect the presence of a Bluetooth device unless it is in the process of actively paging another device. Even if detected, in order to decode more than a few bytes of a message the receiver hop must be in sync with the transmitter. This requires time synchronization to the order of a few tens of microseconds, as well as knowledge of the hopping sequence (determined by the master's device address) and phase of the sequence (determined by the master's Bluetooth clock). This information is delivered to the receiving device at the precise moment the Bluetooth connection is established, and an interceptor that misses this exchange will find it very arduous to sync up with the hopping.

Bluetooth also uses an additional mechanism to improve security. Bluetooth radios have built-in power control mechanisms. This mechanism allows each Bluetooth radio to transmit with only enough power to successfully reach its destination. This is done via a feedback mechanism in which the sending is requested to increase or decrease its transmission power as determined by the receiver's measurements. This is analogous to someone telling another person an important secret, in which a person tends to talk softly to allow only the intended person to hear the secret and does not yell and tell the entire room their secret.

Bluetooth technology provides three modes of security:

[4] For more information on the Frost & Sullivan Bluetooth report, visit frost.com

- *Security mode 1 (non-secure)*. A device does not initiate any security procedure such as encryption or authentication.
- *Security mode 2 (service-level enforcement security)*. A device does not initiate security procedures before channel establishment at the L2CAP (service) level. This mode allows different and flexible access policies for applications, and is used especially for running applications with different security requirements in parallel.
- *Security mode 3 (link-level enforced security)*. A device allows only authenticated connections.

Bluetooth technology provides security infrastructure to deal with not only the open connect-on-the-fly potential for security weaknesses, but provides a breadth and depth of security capabilities to deal with all it's connection models. Bluetooth technology has three security attributes: authorization, authentication, and encryption.

Since there are many services that a Bluetooth device might have, there is a database corresponding to the services a device has authorization to use. The user may be able to choose to "auto" trust devices or "manually" trust devices. Since the identity of the remote device is used as a condition for authorization, authentication is performed. Authentication is accomplished using a challenge-response scheme using symmetric link keys. If the devices do not share a link key, one is created through a process called "pairing" and based on a shared secret association, like a PIN code. If a device does not have a mechanism to enter a PIN, a restricted form link key, called a unit key, is generated based on the device's address and random number. Encryption can only be activated after authentication. Encryption is based on a stream cipher easily implemented in hardware or software.

The Bluetooth security architecture relies on PIN codes for establishing trusted relationships between devices. While not practical to go through all the combinations of uses of PIN codes, it should be noted that once a trusted pairing is established between devices, these codes can be stored within the device to allow more automatic/simple connections. The key to Bluetooth simplicity will be establishing the trusted relationship between commonly used devices. For random ad-hoc connections that require authenticated connections (such as ensuring you are connecting to who you think you are connecting to, something that is not always obvious with invisible radio waves), PINs would have to be exchanged (depending on how the devices are configured).

At a link layer, the Bluetooth radio system provides Authentication, Encryption, and Key Management of the various keys involved. Authentication involves the user providing a Personal Identification Number (PIN) that is translated into a 128-bit link key that can be authenticated in a one- (based from a devices unit key) or two-way direction (combination key). Once the radios are authenticated, the link can be encrypted at various key lengths (up to 128-bits in 8-bit key increments). The link layer security architecture provides a number of authentication schemes and a flexible encryption scheme that allows radios to negotiate for key length. This is important, as radios from different countries will be talking to each other. Security policies in these countries will dictate maximum encryption key lengths. Bluetooth radios will negotiate to the smallest common key length for the link (for example, if a USA radio is enabled for a 128-bit encryption key and a Spanish radio is enabled for only a 48-bit encryption key, the radios will negotiate a link with 48-bit encryption key). The Bluetooth architecture also supports authorization of different services to upper software stacks. For

example, when two computers have created a Bluetooth link to exchange business cards, authorization must be created to extend these services (such that one computer could not examine other services on that computer unless enabled to do so).

4.2.2 Bluetooth Security Concerns and Threats

It seems that for every report that expounds Bluetooth security virtues, there is at least one just as legitimate source reporting concerns about use of Bluetooth as inadequate for serious, security-sensitive work, and lack of strength required for a wireless extension to an enterprise or public network. Even though Bluetooth definitions include security as one of the very most basic and required building blocks of this wireless technology, it is not without some concerns and threats. Large numbers of papers and reports have been published with the intent to analyze Bluetooth security.

Ad hoc Connections

In general terms, there is no fixed infrastructure for ad-hoc networks. Networks are formed on-the-fly, as the name implies. All the devices on a Bluetooth ad hoc network connect to each other via wireless links. Individual devices act as routers when relaying messages to other devices, which may be too far apart from the sending one to get the message directly. The topology of an ad hoc network is not fixed, either. It changes all the time when these mobile devices move in and out of other devices' transmission range. All this makes the ad hoc networks very vulnerable to attacks and the security issues very complicated.

Encryption Key

The security of Bluetooth is based on keeping the encryption key a secret shared only by participants. Encryption is done using a key of length 8- to 128-bits. The length of this key range is necessary purely to accommodate legal requirements in various countries; if legal, 128-bits would normally be used for higher encryption. The encryption key is derived as a byproduct of the authentication process and is entirely different from the authentication key (which is always 128-bits long).

Bluetooth allows for a variety of different encryption keys depending on the scenario. Typically, encryption keys will be different for each session, even in different sessions between the same pair of devices. The only significant exception to this is with encrypted broadcast data, in which case it is desirable for multiple devices to share the same key. The encryption key is based on a so-called “link key,” which may be dynamic or semi-permanent.

In some cases, such as a headset without a user interface, it is preferable to have a semi-permanent link key established automatically and maintained for an indefinite period. This may be accomplished by a process called “bonding.” Two devices to be bonded are brought within wireless range of each other and the process initiated by a means such as pushing a button on one device. The devices initiate a Bluetooth connection with each other, authenticate, establish an encrypted link, and then “pair,” meaning they exchange a pseudo permanent link key for future use. Whenever these two devices connect to each other after this process is complete, they will use the previously exchanged link key to generate a new encryption key for that session. Thus the encryption key changes each time even though the devices are bonded.

A problem arises with the use of the link key. Authentication and encryption are based on the assumption that the link key is the participants' shared secret. All other information used in the procedures is generally public. However this can lead to fundamental problems:

1. Assume that devices **A** and **B** use A's unit key as their link key.
2. Later on, or at the same time, device **C** may communicate with device A and use A's unit key as the link key.
3. **B** uses A's Link key to decrypt the communication between A & C

Device B, having obtained A's unit key earlier, can use the unit key to masquerade as device A and to calculate the encryption key and therefore listen to the traffic. It can also authenticate itself to device A as device C and to device C as device A. This attack is not as easy as it's sounds and requires some work, but was shown to be possible by Lucent Technologies - Bell Labs[5].

Spoofing Bluetooth Device Address

The Bluetooth Device Address is unique to each and every Bluetooth device and is generally programmed into the device at manufacturing time. However this device "uniqueness" brings with it another problem. A special Bluetooth device can be constructed fairly easily that can dynamically re-assign its own device address. Such a device can masquerade or "spoof" another device for purposes of establishing a connection. Once connected, the devices exchange a challenge and response that require the responder share a secret key with the authenticator. Bluetooth requires high-security devices to authenticate in both directions, so that the devices are guaranteed to be who they claim to be. If authentication fails, exponentially increasing waiting periods before retry ensure that the key is not guessed. This challenge/response authentication is based on an algorithm called SAFER+, which is freely available and has been studied extensively by the cryptographic community. This algorithm uses a 128-bit key and is considered extremely secure for this purpose.

Frequency Sniffing

Bluetooth employs frequency hopping spread spectrum technology in the 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band. This band is license-free virtually world-wide, be sniffed easily during this stage. Granted, the window of opportunity is small, but it is an opening nonetheless.

Bluetooth sniffers are already available on the market. CATC, DigiAnswer and Arca-Technologies are three companies that offer such products. These sniffers can pick up transmitted packets directly from the air interface, and log these captured packets for protocol analysis. They are used mainly by developers as a tool to help in their Bluetooth development. On the other hand, this equipment is quite costly, and should be out of reach for common hackers. Although the majority of Bluetooth traffic is encrypted, there are stages of the connection establishment where encryption has not yet been enabled. At this point, such data sniffers can capture link keys used for encryption between device pairs.

---

[5] Jakobsson M., Wetzel S. Security Weakness in Bluetooth: RSA 2001 http://www.bell-labs.com/user/markusj/bt.html

User "Tracking"

Because each Bluetooth device has it's own unique ID, once this ID is associated with a person, individuals can be traced and their activities easily logged, thus personal privacy is violated. This of course is not a data security issue, but a concern nonetheless.

Authenticating Users & Devices: PIN Access

In some usage scenarios, it is desirable to authenticate not only the device but also the user holding the device by requiring the user to enter a PIN code. By sacrificing a level of convenience, this protects against misuse of lost or stolen devices. For these applications, Bluetooth allows a device to prompt the user to enter a PIN number each time a link is established. When the correct PIN is entered, a dynamic encryption key is generated using the PIN and a random number generated by the device. If an invalid PIN is entered, the link is denied.

While some devices will allow the user to punch in an ID number, the PIN can also be stored in the device's memory or on a computer's hard disk. This simplifies the process for the user who needs to use a Bluetooth connection between these same devices frequently, without the annoyance of entering a PIN every time the connection is established. For this convenience, security drops to zero. For many Bluetooth devices they allow user to simple PINs, such as a four digit alpha-numeric PIN. As entering a unique PIN for every Bluetooth connection that requires a PIN (one that cannot be stored in the device), the user may decide to set the PIN to be something simple, easy to remember, and easy to type such as "0000" or "1234". Setting PINs to these simple number sequences makes it very easy to a hacker or virus guess the access PIN to make a connection with your Bluetooth device or PC. Additional using the use of a four digit alpha-numeric PIN is susceptible to brute force and dictionary attacks. This all reduces the certainty of knowing what devices are really connecting to your Bluetooth enabled PC.

4.2.3 Bluetooth Security Recommendations and Solutions

By design, Bluetooth has the potential to replace cables in many current and future connectivity scenarios, and may become a major force in providing short-range personal area networks. As with all wireless communications technologies, all Bluetooth transactions are available to listeners; therefore, Bluetooth needs effective security systems. Bluetooth security systems can be effective, but must be properly implemented, configured, and maintained. Additional security mechanics may be required to be used depending on the sensitivity of the data to be exchanged. The rest of this section describes suggested recommendation and solutions to the security problems that have previously been raises.

PIN access: Implement and enforce strong PINs. When the user is requested to enter a PIN, the user interface should enforce that PIN are of sufficient length (7 or more) with a minimum mixture of upper/lower case, letters, digits, and other special characters.

PIN access: Ensure secure storage of stored PINs or Link Keys. If PINs or Link Keys are store on the device, the storage of this data should be encrypted. This data should be only accessible by another secure method, such as addition PIN, or associated the access to authenticated users accounts, etc.

PIN access: Enforce short PIN life times. Require the user to periodically create new PINs and Link Keys and prevent reuse of the last several used PINs. This should be done frequently enough to prevent continuous security gaps if a user's PIN is discovered.

Spoofing Device ID: Never base authorization on only Device ID: All authorization algorithms should always assume that the Device ID has been spoofed and use therefore other security mechanisms should be used.

Implement strict network access controls. A Bluetooth device may be used to provide short distance, wireless access to a network. A network may offer some simple services to all users, and not require tight security for those services. Allowing free and unregulated access to any network provides an opportunity for unwanted intruders. Knowing that, a network administrator should keep track of who is using the network at all times, requiring some form of network access control. While Bluetooth provides the means for authenticating devices and even users (via a PIN code), this authentication is not suitable for, nor is intended to replace standard network access control.

This problem is really no different than the issues faced when permitting dialup or remote connections to a network. Any access, regardless of how the user establishes the connection, must have strict control policies defined and enforced. Access control such as 802.1x using TLS could be used as needed to enforce highly secure access control.

Use IPSec/ VPNs for encrypted wireless data channels. Just as the recommendation to use IPSEC/VPN for 802.11 wireless LAN access, use of IPSEC/VPN for Bluetooth network traffic is also recommended. Multiple security models are cumbersome to support for multiple connection types. Since most applications today are LAN- and Internet- friendly, an efficient and effective generalization of security is the IPSEC/VPN. IPSEC/VPNs effectively extend the security of a private wired LAN connection out into the world via any combination of dial-up, Internet access, and wireless access – including use of Bluetooth to connect to the network. A VPN provides an end-to-end encryption channel in which the communication is encrypted between the endpoint device and a secure server inside the corporate enterprise. The VPN server, inside the corporate firewall, then forwards the data to the corporate LAN unencrypted, as if the device were locally attached to a wired connection. IPSEC provides addition security, in which the data is encrypted along the entire connection to and from the pair of communicating entities. Bluetooth can be synergistically used in the same manner as end-to-end encryption.

4.3 Wireless WAN

In addition to the dramatic increase in deployments of wireless LANs, the use of wireless wide area networking (WWAN) services is becoming popular as well. As revenue from voice services flattens and voice growth slows among telephony providers, wireless operators (carriers) need to seek additional sources of growth and revenue. Data (packet-switched) services are the next source of growth, as consumers and business users seek richer content, delivered to multiple devices, wherever they are, through these WWAN services. WWAN device cards products are now available on the market to provide such "global connectivity" using a notebook PC.

For public wireless access, the client (notebook, tablet, PDA, smart phone, cell phone, or other device) connects to the Internet via a WWAN carrier such as CDPD, GSM/GPRS, or 2.5G/3G cellular. The client then rides the Internet back to the company, where it authenticates and gains

access to the corporate information by establishing a secure encrypted connection with the network.

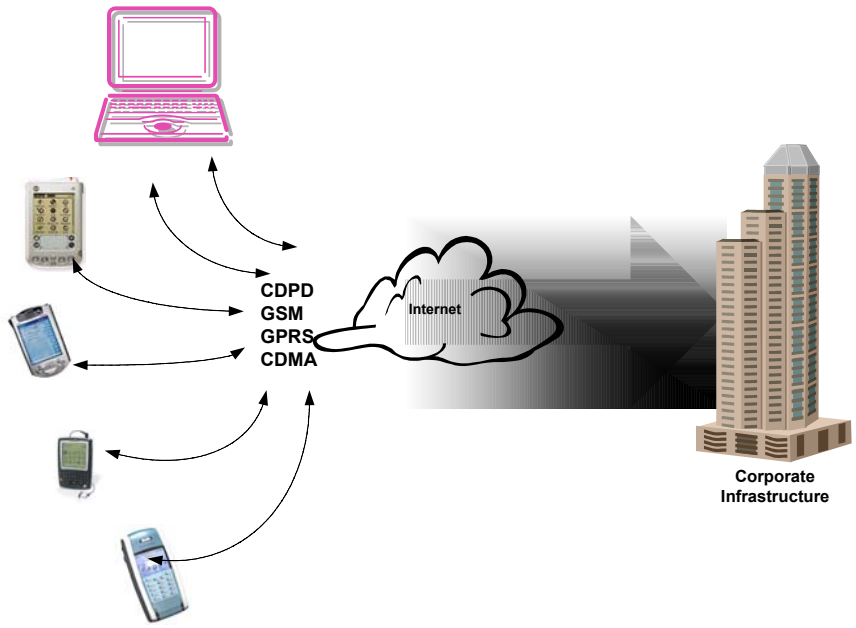


Figure 12: WWAN

WWAN technologies are often characterized by today's deployment of what is termed "2.5G" -- half way between 2nd and 3rd generation. Examples of 2.5G technologies are GPRS and 1xRTT. 3G (third generation) technology is a cellular data transport mechanism that has already arrived in Japan (WCDMA) and will be deployed in the rest of the world starting in the next few years.

WWAN provides packet-data access to the Internet with performance in 30-70kbps range (and getting faster), and is basically built on top of existing 2G networks such as GSM, TDMA, and CDMA. Japan's WCDMA network is similar, but provides well above 200kbps performance.

The critical components in a WWAN environment are:

- **Wireless Gateway.** Provides proxy access for IP-based clients to the other middleware components, such as authentication services, messaging services, and Web and application integration services. The wireless gateway acts as an encryption/decryption and authentication gateway, optimizes IP traffic to reduce overhead, and compresses data to improve the overall client experience.
- **Authentication Services.** Interact with the gateway to provide authentication services for remote clients by validating remote user credentials, interacting with secondary authentication infrastructure, logging all authentication attempts, and suspending any accounts after a configurable number of unsuccessful attempts.

Figure 13 below shows a typical WWAN network. Data flows to/from a client's notebook through the WWAN network, through the Internet and to/from a server for the information at the other end. For the average consumer, this model is sufficient as needs for security are usually limited to protecting credit card and other sensitive information. This type of data can be protected in the network layer using SSL.

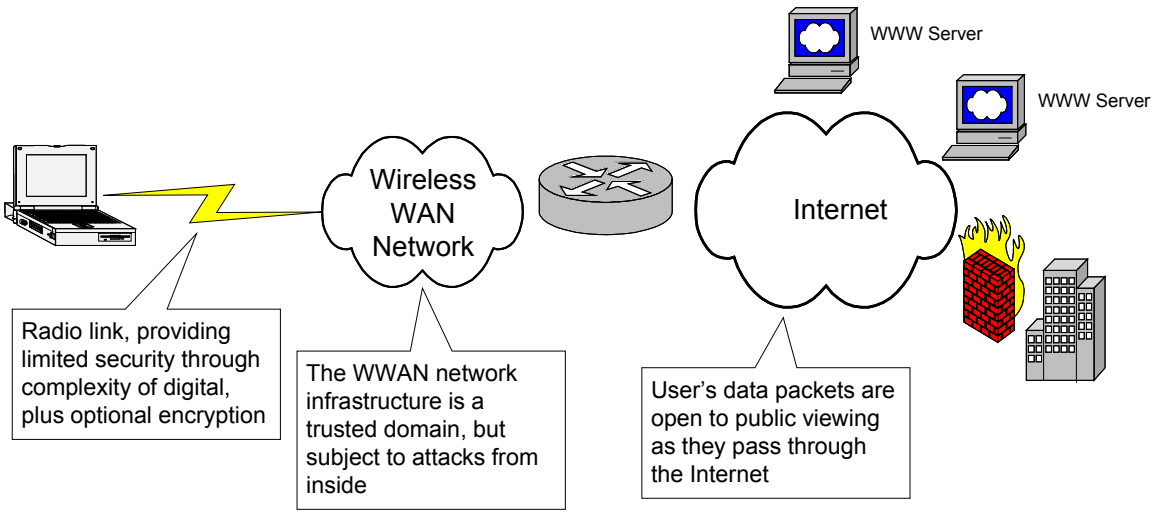


Figure 13: WWAN Access to Corporate Network

For the enterprise user, the model may be insufficient because of the additional need to access corporate resources which may contain highly sensitive information that must be protected. A general network-level security layer is needed to allow clients to access corporate data in the same manner as they do at their desk with the same level of security.

4.3.1 WWAN Security

Many of the same security concerns as discussed for WLAN apply also to WWAN. Terminal equipment used for WAN connections generally are always enabled to provide constant connectivity. With this constant connection, access to GPRS or other types of WAN connections ultimately lead to the Internet which leaves an open door for security concerns such as viruses, Trojans, worms, and other malicious software and hacking threats.

Virtual Private Networks (VPNs)

Demand for data security from eavesdropping over the Internet as well as other points of vulnerability brought about the advent of Virtual Private Networks, which provide secure "tunnels" between any two points, eliminating the points of attack in between.

There are two fundamental ways that VPNs are used with WWAN networks today: Client-to-Enterprise VPNs and Carrier-to-Enterprise VPNs.

Client-to-Enterprise VPNs

Client-to-Enterprise VPNs create an encrypted tunnel between the user's notebook PC and the corporate Intranet. The advantages and disadvantages of Client-to-Enterprise VPNs are listed below:

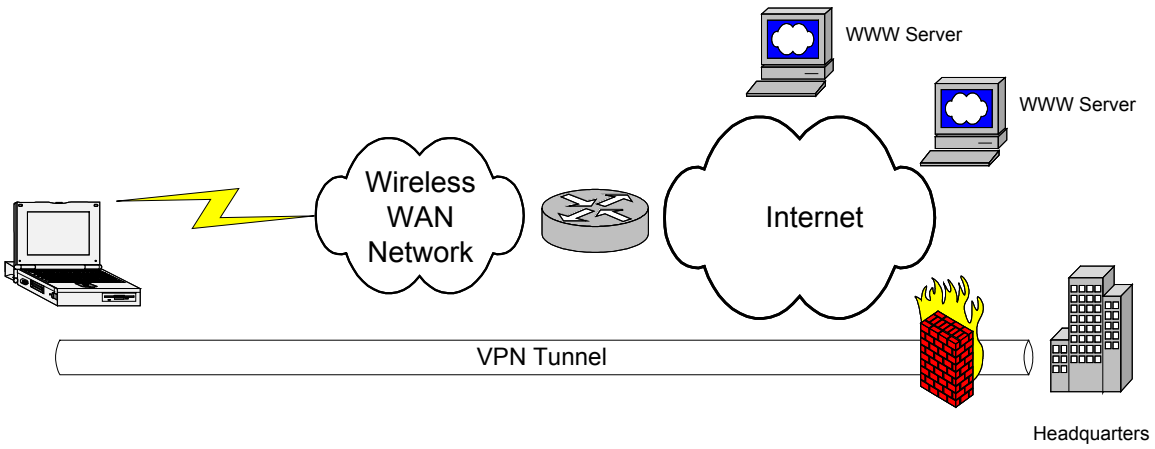


Figure 14: Client to Enterprise VPN

Advantages:

- Eliminates the WWAN air interface, the WWAN network infrastructure, and the Internet as points of attack.
- The entire security solution is controlled by the user or the user's corporate IT. The VPN can be evolved along with the rest of the corporate security strategy.
- One solution fits all. The same VPN can be used across any other Internet-access technology that is used outside of the enterprise. E.g., public or home 802.11, high-speed internet access at hotels.

Disadvantages:

- Requires support by user's IT organization.
- Requires installing and running client VPN software on the user's notebook.
- Requires that the client VPN is compatible with the WWAN network. Well-known problems exist today, such as interoperability with Network Address Translators (NATs). These problems are being addressed but may still be a concern for specific enterprise deployment models.
- Since encrypted data is generally non-compressible, no optimization can take place over the air interface.
- A client-to-enterprise VPN eliminates the ability to use network-provided data acceleration, which is provided by most carriers.
- Client-to-enterprise VPNs introduce an average 20% overhead on data throughput. Therefore a 40kbps average throughput is reduced to 32kbps.

Another type of Carrier-to-Enterprise security solution uses a dedicated connection between the WWAN network and the enterprise, instead of a VPN. Its advantage is guaranteed bandwidth, but at a higher cost.

Overall, the Client-to-Enterprise solution fits most large business needs better than the Carrier-to-Enterprise solution. The primary advantages are end-to-end seamless security, complete control by corporate IT, and scalability across different access technologies.

Carrier-to-Enterprise VPNs

Unlike Client-to-Enterprise VPNs, Carrier-to-Enterprise VPNs only create an encrypted tunnel between the WWAN network and the corporate Intranet. The advantages and disadvantages of Carrier-to-Enterprise VPNs are listed below:

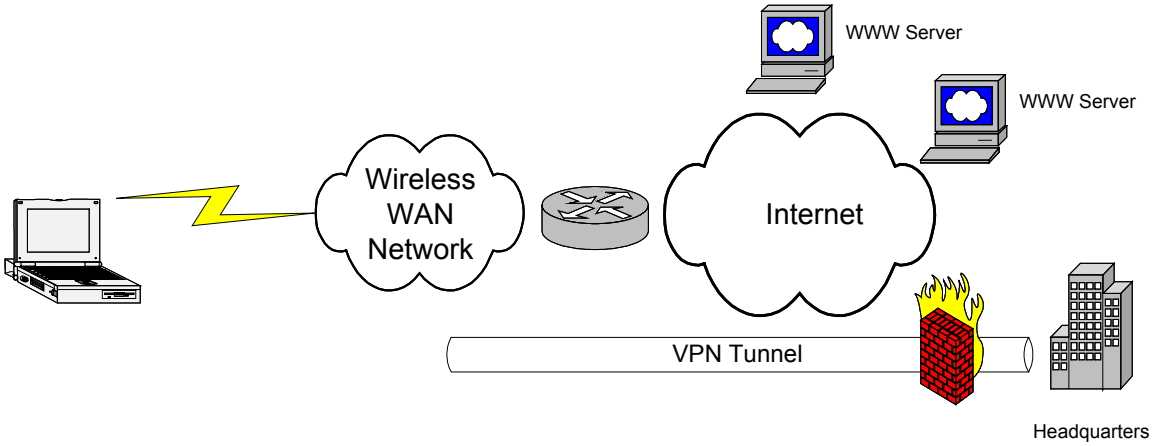


Figure 15: Carrier to Enterprise VPN

Advantages:

- Since managing the VPN is outsourced to the carrier, only minimal support required by the user's IT organization,
- No VPN software need be installed and maintained on the user's notebook.
- Network-VPN compatibility is not an issue.
- One solution fits all. The same VPN can be used across any other Internet-access technology that is used outside of the enterprise. E.g., public or home 802.11, high-speed internet access at hotels.
- User can take advantage of network-provided web acceleration.

Disadvantages:

- The user can only use this VPN solution when access the Internet via WWAN. Other access means such as home or public 802.11 will require a separate security solution.
- Only eliminates the Internet as a potential point of attack. The WWAN air interface and the WWAN network infrastructure remain security threats.
- The user's corporate IT has much less control over the type and adequacy of the VPN used which may not fit well with the corporate security strategy.

4.3.2 WWAN Security Recommendations

Embarking on a WWAN solution is more complicated because the client connects to the Internet via a third-party wireless carrier (CDPD, GSM/GPRS, 2.5G/3G). The client then traverses the Internet back to the company, where it is authenticated and granted access to the corporate information by establishing a secure, encrypted connection with the network. In this scenario, much of the communications link is outside of the control of the corporate IT department.

Problems can occur in this segment of the link including hacking or other malicious mischief that corporate IT cannot prevent.

WWAN provides ~ 30-70kbps packet data access to the Internet, but introduces areas of potential security attacks that need to be addressed in order to access the corporate intranet. Of the security solutions that exist today, the Client-to-Enterprise VPN offers the best solution in most cases as it removes all potential sources of attack between the client's notebook and the enterprise. Client-to-Enterprise VPNs provide the most flexible solution, since they can be used across *any* Internet-access technology with which they are compatible. For these reasons, an increasing number of enterprise users already have a VPN installed on their notebook as issued by corporate IT providers.

For WWAN to be successful in the enterprise, enterprise notebook users must be able to use their existing Client-to-Enterprise VPNs over their WWAN network. For enterprises that prefer carrier-to-enterprise VPNs, there is little or nothing that needs to be done to assure compatibility: there is no client VPN software and any VPN interoperability problems are handled by the WWAN operator.

For deployment, here is a summary of a few tactical guidelines to consider relative to planning and implementing a WWAN:

Require the use of Virtual Private Networking (VPN). Install and configure VPN client software that is optimized for wireless networks and provides cryptography, making it extremely difficult to view the information encapsulated within the resultant "tunnel." If carrier-to-enterprise VPNs are to be used, compatibility must be tested to ensure all the end-to-end pieces deployed work correctly together.

Authentication services to ensure validity of wireless users. Multi-factor authentication mechanisms can help to ensure the user has legitimate claim to a WWAN data connection and can keep hackers from stumbling into open authentication systems. Some of the VPN products on the market have the ability to take advantage of authentication mechanisms including smart cards and biometric devices by using standard MS-CAPI interfaces. Other VPN products have proprietary authentication mechanisms designed to ensure only legitimate users can access WWAN data.

5 Appendix

5.1 Terms & Definitions

Term	Definition
B2B	Business to business – A term used to describe a form of e-commerce between two business entities.
B2C	Business to consumer – A term used to describe e-commerce transactions between a business and a consumer. Most Internet purchases by consumers fit into this classification.
CAPI	Cryptographic Application Programming Interface -- Microsoft Crypto Applications Programming Interface (MS CAPI) is a high-level interface between Windows* applications and a standards-based, core cryptographic functionality. CAPI is a modular software architecture that enables vendors to "plug in" software support for hardware security devices such as smart cards or TPM.
DoS	Denial of service – An attack that attempts to shut down a system or service by flooding it with more requests than it can handle.
Firewall	A method for keeping a network secure from intruders. It can be a single router that filters out unwanted packets or may comprise a combination of routers and servers each performing some type of firewall processing. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise.
IPSec	Internet Protocol Security – A core technology for virtual private networks, IPsec is a set of protocols that supports the secure exchange of packets at the Internet Protocol (IP) layer.
PC/SC	Personal Computer / Smart Card – An architecture that enables Smart Cards to be utilized on a variety of systems, such as Windows* PCs. It is designed to support a high degree of vendor independence and to promote interoperability amongst products, whether they are smart cards, tokens or reader/devices.
PIN	Personal Identification Number – a form of password often used to gain access to personal or private information. A PIN is used to unlock secret information stored in a smart card.

Term	Definition
PKCS	Public-Key Cryptography Standards – A family of security related standards offered by RSA Laboratories
PKCS#11	PKCS#11 is a medium-level, hardware-independent token interface developed by RSA Data Security, Inc. and its licensees. It is a commonly adopted interface being used by PKI vendors, e.g. Baltimore, Entrust, RSA/Xcert, TC TrustCentre, Verisign and WiseKey to integrate hardware tokens for Digital Certificates, key storage and generation. PKCS #11 is also sometimes referred to as Cryptoki.
PKI	Public Key Infrastructure – Technology for managing digital certificates and encryption keys.
Spoofing	Pretending to be another system or individual.
SSL	Secure Sockets Layer – A major security protocol used to provide a secure connection on the Internet. When an SSL session is started, the server sends its public key to the browser, which the browser uses to send a randomly generated secret key back to the server in order to have a secret key exchange for that session. Developed by Netscape, SSL has been merged with other protocols and authentication methods by the IETF into a new protocol known as Transport Layer Security (TLS).
TCPA	Trusted Computing Platform Alliance – an industry organization self chartered to provide security related architecture for the computer industry.
TKIP	Temporal Key Integrity Protocol – Part of the 802.11i proposal for improved encryption.
TLS	Transport Layer Security – A security protocol from the IETF that is a merger of SSL and other protocols. TLS is backward compatible with SSL and uses Triple DES encryption.
TPM	Trusted Platform Module – A hardware security device defined by the TCPA to provide secure, non-volatile storage for security keys and certificates, hashing and encryption algorithms and other security related features.
Trojan horse	A backdoor program or bad code that allows unauthorized access to your computer.

Term	Definition
Virus	A small program designed to perform a malicious task that attaches itself to another program.
VPN	Virtual Private Network – A secure private network "tunnel" that is configured to be used over a public network such as the Internet. Data sent through a VPN connection is encrypted from end-to-end, thus providing a secure pathway for data going from an end user into a corporate enterprise network.
Worm	A virus that is self-replicating.

5.2 References

- "Batten Down the Security Hatches" by Helen D'Antoni, Information Week, May 13, 2002. http://www.informationweek.com/story/IWK20020509S0003
- "Building the Foundation for Anytime, Anywhere Computing", Intel white paper, Document number: 251290-002 06/13, http://www.intel.com/ebusiness/pdf/it/pp022402.pdf
- "Enterprise Security and the Importance of Authorization Technology", Intel white paper, Document # 298537-001, http://www.intel.com/ebusiness/pdf/bestpractices/wp013606.pdf
- "Getting Connected without Wires", Intel white paper, http://www.intel.com/network/connectivity/products/getting_connected.htm
- "How High Performance PCs Can Enhance Information Security", Intel white paper, Document #250951-001, http://www.intel.com/ebusiness/pdf/prod/desktop/p4p/ar021801.pdf
- "Integrating Bluetooth* Technology into Mobile Products", Intel white paper, Graham Kirby, Q2'2000, http://www.intel.com/technology/itj/q22000/articles/art_4.htm
- "Intel 802.11b Networking for Large Organizations", Intel white paper, http://www.intel.com/network/connectivity/resources/doc_library/data_sheets/NP169003.pdf
- "Overview of 802.11 Security", Q2'2000, Sultan Weatherspoon, Intel white paper, http://www.intel.com/technology/itj/q22000/articles/art_5.htm

- "Wide Area Networking", Intel white paper, http://www.intel.com/network/connectivity/resources/doc_library/white_papers/wide_area.htm

- "Wireless 802.11 Security in a Corporate Environment", Intel white paper, http://www.intel.com/ebusiness/products/related_mobile/wp012602.htm

- "Wireless Security and VPN", Intel white paper, Document Number: NP2045.01, http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/WLO_Security_WP_LOWrez1.pdf

- "Your 802.11 Wireless Network Has No Clothes", Scott Fluhrer, Itsik Mantin, and Adi Shamir, March 30, 2001. http://www.cs.umd.edu/~waa/wireless.pdf

- ANSI/IEEE Std 802.11, 1999 Edition – Part 11: Wireless LAN Medium Access and Control (MAC) and Physical Layer (PHY) Specifications

- Bluetooth, The Bluetooth Specification, v.1.0B http://www.bluetooth.com/developer/specification/specification.asp

- *Removable Security Device: Vendor Recommendations*, Intel Corporation, Version 0.9, July 2002, Document Number: 12014.

- RSA Laboratories PKCS #11 v2.10: Cryptographic Token Interface Standard. (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/)

- *Trusted Platform Module (TPM) based Security on Notebook PCs* – Intel white paper, Intel Corporation, June 2002.

- *Trusted Platform Module: Vendor Recommendations*, Intel Corporation, Version 1.00, June 2002, Document Number: 11589.